PCT/JP2004/005528

日本国特許庁
JAPAN PATENT OFFICE

14.4.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月２４日

出願番号
Application Number: 特願２００３－１１９９７３

[ST. 10/C]: [ＪＰ２００３－１１９９７３]

出願人
Applicant(s): 松下電器産業株式会社

２００４年　５月２８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０４５５９７

【書類名】　特許願
【整理番号】　2022550083
【提出日】　平成15年 4月24日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　5/00
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　山道　将人
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　布田　裕一
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　大森　基司
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　館林　誠
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100097445
【弁理士】
【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　パラメータ生成装置、パラメータ変換装置、暗号化システム、復号化システム、暗号装置、復号装置、暗号化方法、復号化方法、及びコンピュータ読取可能な記録媒体

【特許請求の範囲】

【請求項１】　外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成する出力パラメータ生成部と、

を備えることを特徴とする、パラメータ生成装置。

【請求項２】　前記出力パラメータ生成部は、前記格子強度係数に基づく安全性決定情報と前記安全性レベル情報に基づいて、前記仮パラメータ組から前記出力パラメータを生成することを特徴とする、請求項１に記載のパラメータ生成装置。

【請求項３】　前記出力パラメータ生成部は、前記安全性決定情報を保持する安全性決定情報保持手段を備え、前記安全性決定情報は、外部より与えられることを特徴とする、請求項２に記載のパラメータ生成装置。

【請求項４】　前記仮パラメータ組及び前記出力パラメータは、ＮＴＲＵ暗号における次元Ｎ、非負整数ｐ、非負整数ｑ、秘密鍵多項式ｆにおける係数の値が１となる係数の数を規定する非負整数ｄｆ、公開鍵多項式を生成するときに用いるランダム多項式ｇの係数の値が１となる係数の数を規定する非負整数ｄｇ、及び平文を暗号化する時に用いる乱数多項式ｒの係数の値が１となる係数の数を規定する非負整数ｄの組から構成されることを特徴とする、請求項１から請求項３のいずれか１項に記載のパラメータ生成装置。

【請求項５】　前記仮パラメータ生成部は、初期安全性決定情報を保持する初期安全性決定情報保持手段を備え、前記安全性レベル情報と前記初期安全性決定情報に基づいて前記仮パラメータ組に含まれる前記次元Ｎを生成することを特徴とする、請求項４に記載のパラメータ生成装置。

【請求項６】　前記仮パラメータ生成部は、前記安全性レベル情報と前記次元Ｎに基づいて前記仮パラメータ組に含まれる前記非負整数ｄｆ、前記非負整数ｄｇ、前記非負整数ｄを生成することを特徴とする、請求項４または請求項５に記載のパラメータ生成装置。

【請求項７】　前記仮パラメータ生成部は、前記エラー条件情報に基づいて前記仮パラメータ組に含まれる前記非負整数ｑを生成することを特徴とする、請求項４から請求項６のいずれか１項に記載のパラメータ生成装置。

【請求項８】　前記出力パラメータ生成部は、前記安全性レベル情報と前記安全性決定情報に基づいて前記出力パラメータ組に含まれる前記次元Ｎを生成することを特徴とする、請求項４から請求項７のいずれか１項に記載のパラメータ生成装置。

【請求項９】　前記エラー条件情報は、復号エラーが発生しないための条件を表す条件式であることを特徴とする、請求項１から請求項８のいずれか１項に記載のパラメータ生成装置。

【請求項１０】　前記エラー条件情報は、前記非負整数ｐ、前記非負整数ｑ、前記非負整数ｄ、前記非負整数ｄｆに対し、復号エラーが発生しないための条件を表す条件式

$$2 \cdot p \cdot d + 2df - 1 < q / 2$$

であることを特徴とする、請求項１から請求項９のいずれか１項に記載のパラメータ生成装置。

【請求項１１】　前記出力パラメータ生成部は、１つ以上の格納格子強度係数と格納安全性決定情報の組を格納する格子強度係数格納手段を備え、

前記格納格子強度係数と格納安全性決定情報は、外部から与えられることを特徴とする、請求項２から請求項１０のいずれか１項に記載のパラメータ生成装置。

【請求項１２】　前記出力パラメータ生成部は、さらに、前記格子強度係数に基づいて前記格納安全性決定情報から、前記安全性決定情報を選択する安全性決定情報選択手段を備えることを特徴とする、請求項１１に記載のパラメータ生成装置。

【請求項１３】　前記出力パラメータ生成部は、前記格子強度係数と前記格納格子強度係数に基づいて前記仮パラメータ組を変更するか否かを判定する変更判定手段と、前記変更手段の判定に基づき、前記仮パラメータ組から変更仮パラメータ組を生成する仮パラメータ組変更手段を備え、前記安全性レベル情報に基づいて前記変更仮パラメータ組から前記出力パラメータを生成することを特徴とする、請求項１１に記載のパラメータ生成装置。

【請求項１４】　前記仮パラメータ変更手段は、前記仮パラメータ組の前記非負整数ｄｇを変更して前記変更仮パラメータ組を生成することを特徴とする、請求項１３に記載のパラメータ生成装置。

【請求項１５】　外部から入力された安全性レベル情報に基づき、外部から入力されたＮＴＲＵ暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータに変換して出力するパラメータ変換装置であって、

前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成する出力パラメータ生成部と、

を備えることを特徴とする、パラメータ変換装置。

【請求項１６】　前記出力パラメータ生成部は、前記格子強度係数に基づく安全性決定情報と前記安全性レベル情報に基づいて、前記仮パラメータ組から前記出力パラメータを生成することを特徴とする、請求項１５に記載のパラメータ変換装置。

【請求項１７】　前記出力パラメータ生成部は、前記安全性決定情報を保持する安全性決定情報保持手段を備え、前記安全性決定情報は、外部より与えられることを特徴とする、請求項１６に記載のパラメータ変換装置。

【請求項１８】　前記仮パラメータ組及び前記出力パラメータは、ＮＴＲＵ暗号における次元Ｎ、非負整数ｐ、非負整数ｑ、秘密鍵多項式ｆにおける係数の値が１となる係数の数を規定する非負整数ｄｆ、公開鍵多項式を生成するときに用いるランダム多項式ｇの係数の値が１となる係数の数を規定する非負整数ｄｇ、及び平文を暗号化する時に用いる乱数多項式ｒの係数の値が１となる係数の数を規定する非負整数ｄの組から構成されることを特徴とする、請求項１５から請求項１７のいずれか１項に記載のパラメータ変換装置。

【請求項１９】　前記仮パラメータ生成部は、前記エラー条件情報に基づいて前記仮パラメータ組に含まれる前記非負整数ｑを生成することを特徴とする、請求項１８に記載のパラメータ変換装置。

【請求項２０】　前記出力パラメータ生成部は、前記安全性レベル情報と前記安全性決定情報に基づいて前記出力パラメータ組に含まれる前記次元Ｎを生成することを特徴とする、請求項１８または請求項１９に記載のパラメータ変換装置。

【請求項２１】　前記エラー条件情報は、復号エラーが発生しないための条件を表す条件式であることを特徴とする、請求項１５から請求項２０のいずれか１項に記載のパラメータ変換装置。

【請求項２２】　前記エラー条件情報は、前記非負整数ｐ、前記非負整数ｑ、前記非負整数ｄ、前記非負整数ｄｆに対し、復号エラーが発生しないための条件を表す条件式

$$2 \cdot p \cdot d + 2 \cdot df - 1 < q / 2$$

であることを特徴とする、請求項１５から請求項２１のいずれか１項に記載のパラメータ変換装置。

【請求項２３】　前記出力パラメータ生成部は、１つ以上の格納格子強度係数と格納安全性決定情報の組を格納する格子強度係数格納手段を備え、

前記格納格子強度係数と格納安全性決定情報は、外部から与えられることを特

徴とする、請求項１６から請求項２２のいずれか１項に記載のパラメータ変換装置。

【請求項２４】　前記出力パラメータ生成部は、さらに、前記格子強度係数に基づいて前記格納安全性決定情報から、前記安全性決定情報を選択する安全性決定情報選択手段を備えることを特徴とする、請求項２３に記載のパラメータ変換装置。

【請求項２５】　前記出力パラメータ生成部は、前記格子強度係数と前記格納格子強度係数に基づいて前記仮パラメータ組を変更するか否かを判定する変更判定手段と、前記変更手段の判定に基づき、前記仮パラメータ組から変更仮パラメータ組を生成する仮パラメータ組変更手段を備え、前記安全性レベル情報に基づいて前記変更仮パラメータ組から前記出力パラメータを生成することを特徴とする、請求項２３に記載のパラメータ変換装置。

【請求項２６】　前記仮パラメータ変更手段は、前記仮パラメータ組の前記非負整数ｄｇを変更して前記変更仮パラメータ組を生成することを特徴とする、請求項２５に記載のパラメータ変換装置。

【請求項２７】　外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の暗号鍵と復号鍵を生成して出力する鍵生成装置と、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号装置と、前記暗号文を復号した復号文を生成して出力する復号装置とから構成される暗号化システムであって、

前記パラメータ生成装置は、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵と前記復号鍵を生成し出力する生成鍵出力部を備え、

前記暗号装置は、

前記パラメータ生成装置が出力した出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備え、

前記復号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする、暗号化システム。

【請求項２８】　外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の暗号鍵を生成して出力する鍵生成装置と、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号装置とから構成される暗号化システムであって、

前記パラメータ生成装置は、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵を生成し出力する生成鍵出力部を備え、

前記暗号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備えることを特徴とする、暗号化システム。

【請求項２９】　外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して復号装置へ送信する暗号装置であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力する出力パラメータ生成部と、

前記出力パラメータを前記復号装置へ送信するパラメータ送信部と、

前記復号装置から前記出力パラメータに基づいて生成されたＮＴＲＵ暗号の暗号鍵を受信する暗号鍵受信部と、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して前記暗号文を生成して送信する暗号文送信部を備えることを特徴とする、暗号装置。

【請求項３０】　外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号化方法であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてＮＴＲＵ暗号の暗号鍵を生成するステップと、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを含むことを特徴とする、暗号化方法。

【請求項３１】　外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてＮＴＲＵ暗号の暗号鍵を生成するステップと、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを、コンピュータに実行させることを特徴とするプログラムを記録した記録媒体。

【請求項３２】　外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の復号鍵を生成して出力する鍵生成装置と、外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号装置とから構成される復号化システムであって、

前記パラメータ生成装置は、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記復号鍵を生成し出力する生成鍵出力部を備え、

前記復号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出

力する復号化部を備えることを特徴とする、復号化システム。

【請求項３３】　暗号装置から受信した暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号装置であって、

前記暗号装置から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを受信するパラメータ受信部と、

前記出力パラメータを入力としてＮＴＲＵ暗号の暗号鍵と復号鍵を生成し出力する生成鍵出力部と、

前記暗号鍵を前記暗号装置へ送信する暗号鍵送信部と、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して前記復号文を生成して出力する復号文生成部を備えることを特徴とする、復号装置。

【請求項３４】　外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号化方法であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてＮＴＲＵ暗号の復号鍵を生成するステップと、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを含むことを特徴とする、復号化方法。

【請求項３５】　外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、

予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてＮＴＲＵ暗号の復号鍵を生成するステップと、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを、コンピュータに実行させることを特徴とするプログラムを記録した記録媒体。

【請求項３６】　外部から入力された安全性レベル情報に基づき、外部から入力されたＮＴＲＵ暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータに変換して出力するパラメータ変換装置と、ＮＴＲＵ暗号の暗号鍵と復号鍵を生成して出力する鍵生成装置と、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号装置と、前記暗号文を復号した復号文を生成して出力する復号装置とから構成される暗号システムであって、

前記パラメータ変換装置は、

前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵と前記復号鍵を生成し出力する生成鍵出力部を備え、

前記暗号装置は、

前記パラメータ生成装置が出力した出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力す

る暗号化部を備え、

前記復号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする、暗号システム。

【請求項３７】　外部から入力された安全性レベル情報に基づき、外部から入力されたＮＴＲＵ暗号のパラメータ組である入力パラメータと、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の暗号鍵を生成して出力する鍵生成装置と、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号装置とから構成される暗号化システムであって、

前記パラメータ生成装置は、

前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵を生成し出力する生成鍵出力部を備え、

前記暗号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備えることを特徴とする、暗号化システム。

【請求項３８】　外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して復号装置へ送信する暗号装置であって、

予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与え

られた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力する出力パラメータ生成部と、

前記出力パラメータを前記復号装置へ送信するパラメータ送信部と、

前記復号装置から前記出力パラメータに基づいて生成されたＮＴＲＵ暗号の暗号鍵を受信する暗号鍵受信部と、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して前記暗号文を生成して送信する暗号文送信部を備えることを特徴とする、暗号装置。

【請求項３９】　外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号化方法であって、

予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてＮＴＲＵ暗号の暗号鍵を生成するステップと、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを含むことを特徴とする、暗号化方法。

【請求項４０】　外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、

予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与え

られた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてＮＴＲＵ暗号の暗号鍵を生成するステップと、

前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを、コンピュータに実行させることを特徴とするプログラムを記録した記録媒体。

【請求項４１】　外部から入力された安全性レベル情報に基づき、外部から入力されたＮＴＲＵ暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の復号鍵を生成して出力する鍵生成装置と、外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号装置とから構成される復号化システムであって、

前記パラメータ生成装置は、

前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、

前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、

前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、

前記鍵生成装置は、

前記パラメータ生成装置が出力した前記出力パラメータを入力として前記復号鍵を生成し出力する生成鍵出力部を備え、

前記復号装置は、

前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする、復号化システム。

【請求項４２】　外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号化方法であって、

予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてＮＴＲＵ暗号の復号鍵を生成するステップと、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを含むことを特徴とする、復号化方法。

【請求項４３】　外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、

予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、

前記仮パラメータ組から格子強度係数を計算するステップと、

前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、

前記出力パラメータに基づいてＮＴＲＵ暗号の復号鍵を生成するステップと、

前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を

生成して出力するステップとを、コンピュータに実行させることを特徴とするプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、ＮＴＲＵ暗号のパラメータ生成に関するものである。

【０００２】

【従来の技術】

送信装置と受信装置との間で秘匿通信を実現する方法として、公開鍵暗号を用いた暗号化通信がある。簡単に説明すると、送信装置が、通信内容を受信装置の公開鍵を用いて暗号化して送信し、受信装置は、暗号化された通信内容を受信し、それを自身の秘密鍵を用いて復号して元の通信内容を得る方法である（例えば、非特許文献１参照）。この方法を用いる一般的な暗号システムでは、送信装置及び受信装置は、ともに複数存在する。まず、送信装置は、通信先受信装置の公開鍵を取得する。この公開鍵は、通信先受信装置が有する秘密鍵と対になるものでありシステムにおいて公開されている。そして、送信装置は、通信すべきデータ内容を上記のように取得した公開鍵で暗号化して送信する。一方で、受信装置は、上記のように暗号化された通信内容データを受信する。そして、受信装置は、暗号化された通信内容データを、自身の有する秘密鍵で復号して元の通信内容データを得る。

【０００３】

なお、暗号は、送信装置と受信装置との間の秘匿通信を目的とするものであり、第三者による暗号解読に対する安全性が重要なのは言うまでもない。公開鍵暗号では、暗号化された通信内容データ（以降、暗号文と記述）から、通信内容データ（以降、平文と記述）が解読される可能性と、受信装置が秘密に保持し、暗号文から平文を得る際に用いる秘密鍵が解読される可能性がある。一般に、公開鍵暗号では、第三者によるこれらの暗号解読の解読時間が十分に大きく（例えば、最新のコンピュータを用いて１０００年かかる等）、現実的な時間内では解読

できないことが求められる。

【０００４】

１９９６年、高速処理が可能な公開鍵暗号として、ＮＴＲＵ暗号が提案された（例えば、非特許文献２参照）。このＮＴＲＵ暗号については、非特許文献２に詳細が記載されているのでここでは詳細な説明を省略するが、ある法の下でべき乗剰余演算を行うＲＳＡ暗号や楕円曲線上の点のスカラ倍演算を行う楕円曲線暗号に比べ、高速に演算可能な多項式演算で暗号化と復号化を行うので、従来の公開鍵暗号よりもソフトウェアにより高速に処理することが可能である。

【０００５】

従って、公開鍵暗号にＮＴＲＵ暗号を用いた暗号システムでは、従来の公開鍵暗号を用いた暗号システムよりも、送信装置及び受信装置の処理が高速に行えるという利点がある。

【０００６】

なお、このＮＴＲＵ暗号を用いて実際に暗号化や復号化を行うためには、非負整数のパラメータ、Ｎ、ｐ、ｑ、ｄｆ、ｄｇ、ｄが必要であり（例えば、非特許文献２参照）、現在、これらのパラメータの具体的な値が提示されている（例えば、非特許文献５参照）。

【０００７】

このＮＴＲＵ暗号は、第三者による平文や秘密鍵の暗号解読方法として、これらを総当りで探索する暗号解読と、ＬＬＬアルゴリズムを用いて解読する暗号解読がある（例えば、非特許文献２参照）が、非特許文献５に提示されたパラメータを用いれば、これらの暗号解読の解読時間は十分に大きく、ＮＴＲＵ暗号は安全であることが示されている（例えば、非特許文献３、非特許文献４、非特許文献５参照）。

【０００８】

一方、このＮＴＲＵ暗号は、公開鍵を用いて平文を暗号化して暗号文を生成し、正規の秘密鍵を用いて暗号文を復号して復号文を生成しても、復号文が元の平文と異なる場合が発生する（例えば、非特許文献２参照）。このことを復号エラーが発生するという。この復号エラーはＮＴＲＵ暗号のパラメータにより、その

発生確率が異なる（例えば、非特許文献５参照）。

【０００９】

この復号エラーに関し、非特許文献２には、復号エラーが発生しないためには、ＮＴＲＵ暗号の公開鍵多項式ｈを生成するときに用いるランダム多項式ｇ、乱数多項式ｒ、平文多項式ｍ、秘密鍵多項式ｆの演算結果の多項式（ｐ・ｒ×ｇ＋ｆ×ｍ）の係数の値が－ｑ／２からｑ／２に入ることが必要であることが示されている。しかし、このようにＮＴＲＵ暗号のパラメータを選んだときの暗号解読に対する解読時間については不明であり、暗号解読に対して安全でかつ復号エラーが発生しないＮＴＲＵ暗号のパラメータは知られていない。

【００１０】

【非特許文献１】

岡本龍明、山本博資、「現代暗号」、シリーズ／情報科学の数学、産業図書、１９９７.

【非特許文献２】

Jeffery Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998.

【非特許文献３】

Joseph H. Silverman, "NTRU Cryptosystems Technical Report #012, Estimated Breaking Times for NTRU Lattices", [online]、1999年3月9日、[2003年2月18日検索]、インターネット<URL: http://www.ntru.com/cryptolab/pdf/NTRUTech012.pdf>

【非特許文献４】

Joseph H. Silverman, "NTRU Cryptosystems Technical Report #013, Dimension-Reduced Lattices, Zero-Forced Lattices, and the NTRU Public Key Cryptosystem", [online]、1999年3月9日、[2003年2月18日検索]、インターネット<URL: http://www.ntru.com/cryptolab/pdf/NTRUTech013.pdf>

【非特許文献５】

Joseph H. Silverman, ”NTRU Cryptosystems Technical Report #011, Wraps, Gaps, and Lattice Constants”, [online]、1999年1月21日、[2003年4月18日検索]、インターネット<URL: http://www.ntru.com/cryptolab/pdf/NTRUTech011#v2.pdf>

【００１１】

【発明が解決しようとする課題】

上述したように、高速処理が可能なＮＴＲＵ暗号では、復号エラーが発生すると、受信装置が、送信装置の暗号化した平文を正しく得られない場合がある。すなわち、送信装置と受信装置との間で確実な暗号化通信ができないことになる。

【００１２】

暗号システムにおいては、平文を相手に正しく伝えることが重要なのは言うまでもない。また、暗号は、第三者による暗号解読に対する安全性が重要なのは言うまでもない。

【００１３】

しかしながら、従来の技術では、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータを生成するための条件が知られておらず、そのようなＮＴＲＵ暗号のパラメータを生成できない。そのため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができない。

【００１４】

そこで、本発明は上記の課題に鑑み、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるように、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータを生成するパラメータ生成装置を提供することを第１の目的とする。

【００１５】

また、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるように、入力されたＮＴＲＵ暗号のパラメータに対し、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータに変換するパラメータ変換装置を提供することを第２の目的とする。

【００１６】

また、これらのパラメータ装置もしくはパラメータ変換装置により生成されたパラメータを用いて、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができる、暗号システム、暗号装置及び復号装置を提供することを第３の目的とする。

【００１７】

【課題を解決するための手段】

上記課題を解決するために、請求項１における発明は、外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成する出力パラメータ生成部とを備えることを特徴とする。

【００１８】

請求項２における発明は、請求項１に記載のパラメータ生成装置において、前記出力パラメータ生成部は、前記格子強度係数に基づく安全性決定情報と前記安全性レベル情報に基づいて、前記仮パラメータ組から前記出力パラメータを生成することを特徴とする。

【００１９】

請求項３における発明は、請求項２に記載のパラメータ生成装置において、前記出力パラメータ生成部は、前記安全性決定情報を保持する安全性決定情報保持手段を備え、前記安全性決定情報は、外部より与えられることを特徴とする。

【００２０】

請求項４における発明は、請求項１から請求項３のいずれか１項に記載のパラメータ生成装置において、前記仮パラメータ組及び前記出力パラメータは、ＮＴＲＵ暗号における次元Ｎ、非負整数ｐ、非負整数ｑ、秘密鍵多項式ｆにおける係数の値が１となる係数の数を規定する非負整数ｄｆ、公開鍵多項式を生成すると

きに用いるランダム多項式ｇの係数の値が１となる係数の数を規定する非負整数ｄｇ、及び平文を暗号化する時に用いる乱数多項式ｒの係数の値が１となる係数の数を規定する非負整数ｄの組から構成されることを特徴とする。

【００２１】

請求項５における発明は、請求項４に記載のパラメータ生成装置において、前記仮パラメータ生成部は、初期安全性決定情報を保持する初期安全性決定情報保持手段を備え、前記安全性レベル情報と前記初期安全性決定情報に基づいて前記仮パラメータ組に含まれる前記次元Ｎを生成することを特徴とする。

【００２２】

請求項６における発明は、請求項４または請求項５に記載のパラメータ生成装置において、前記仮パラメータ生成部は、前記安全性レベル情報と前記次元Ｎに基づいて前記仮パラメータ組に含まれる前記非負整数ｄｆ、前記非負整数ｄｇ、前記非負整数ｄを生成することを特徴とする。

【００２３】

請求項７における発明は、請求項４から請求項６のいずれか１項に記載のパラメータ生成装置において、前記仮パラメータ生成部は、前記エラー条件情報に基づいて前記仮パラメータ組に含まれる前記非負整数ｑを生成することを特徴とする。

【００２４】

請求項８における発明は、請求項４から請求項７のいずれか１項に記載のパラメータ生成装置において、前記出力パラメータ生成部は、前記安全性レベル情報と前記安全性決定情報に基づいて前記出力パラメータ組に含まれる前記次元Ｎを生成することを特徴とする。

【００２５】

請求項９における発明は、請求項１から請求項８のいずれか１項に記載のパラメータ生成装置において、前記エラー条件情報は、復号エラーが発生しないための条件を表す条件式であることを特徴とする。

【００２６】

請求項１０における発明は、請求項１から請求項９のいずれか１項に記載のパ

ラメータ生成装置において、前記エラー条件情報は、前記非負整数ｐ、前記非負整数ｑ、前記非負整数ｄ、前記非負整数ｄｆに対し、復号エラーが発生しないための条件を表す条件式２・ｐ・ｄ＋２ｄｆ－１＜ｑ／２であることを特徴とする。

【００２７】

請求項１１における発明は、請求項２から請求項１０のいずれか１項に記載のパラメータ生成装置において、前記出力パラメータ生成部は、１つ以上の格納格子強度係数と格納安全性決定情報の組を格納する格子強度係数格納手段を備え、前記格納格子強度係数と格納安全性決定情報は、外部から与えられることを特徴とする。

【００２８】

請求項１２における発明は、請求項１１に記載のパラメータ生成装置は、前記出力パラメータ生成部において、さらに、前記格子強度係数に基づいて前記格納安全性決定情報から、前記安全性決定情報を選択する安全性決定情報選択手段を備えることを特徴とする。

【００２９】

請求項１３における発明は、請求項１１に記載のパラメータ生成装置において、前記出力パラメータ生成部は、前記格子強度係数と前記格納格子強度係数に基づいて前記仮パラメータ組を変更するか否かを判定する変更判定手段と、前記変更手段の判定に基づき、前記仮パラメータ組から変更仮パラメータ組を生成する仮パラメータ組変更手段を備え、前記安全性レベル情報に基づいて前記変更仮パラメータ組から前記出力パラメータを生成することを特徴とする。

【００３０】

請求項１４における発明は、請求項１３に記載のパラメータ生成装置において、前記仮パラメータ変更手段は、前記仮パラメータ組の前記非負整数ｄｇを変更して前記変更仮パラメータ組を生成することを特徴とする。

【００３１】

請求項１５における発明は、外部から入力された安全性レベル情報に基づき、外部から入力されたＮＴＲＵ暗号のパラメータ組である入力パラメータを、前記

安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータに変換して出力するパラメータ変換装置であって、前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成する出力パラメータ生成部と、を備えることを特徴とする。

【００３２】

請求項１６における発明は、請求項１５に記載のパラメータ変換装置において、前記出力パラメータ生成部は、前記格子強度係数に基づく安全性決定情報と前記安全性レベル情報に基づいて、前記仮パラメータ組から前記出力パラメータを生成することを特徴とする。

【００３３】

請求項１７における発明は、請求項１６に記載のパラメータ変換装置において、前記出力パラメータ生成部は、前記安全性決定情報を保持する安全性決定情報保持手段を備え、前記安全性決定情報は、外部より与えられることを特徴とする。

【００３４】

請求項１８における発明は、請求項１５から請求項１７のいずれか１項に記載のパラメータ変換装置において、前記仮パラメータ組及び前記出力パラメータは、ＮＴＲＵ暗号における次元Ｎ、非負整数ｐ、非負整数ｑ、秘密鍵多項式ｆにおける係数の値が１となる係数の数を規定する非負整数ｄｆ、公開鍵多項式を生成するときに用いるランダム多項式ｇの係数の値が１となる係数の数を規定する非負整数ｄｇ、及び平文を暗号化する時に用いる乱数多項式ｒの係数の値が１となる係数の数を規定する非負整数ｄの組から構成されることを特徴とする。

【００３５】

請求項１９における発明は、請求項１８に記載のパラメータ変換装置において、前記仮パラメータ生成部は、前記エラー条件情報に基づいて前記仮パラメータ

組に含まれる前記非負整数ｑを生成することを特徴とする。

【００３６】

請求項２０における発明は、請求項１８または請求項１９に記載のパラメータ変換装置において、前記出力パラメータ生成部は、前記安全性レベル情報と前記安全性決定情報に基づいて前記出力パラメータ組に含まれる前記次元Ｎを生成することを特徴とする。

【００３７】

請求項２１における発明は、請求項１５から請求項２０のいずれか１項に記載のパラメータ変換装置において、前記エラー条件情報は、復号エラーが発生しないための条件を表す条件式であることを特徴とする。

【００３８】

請求項２２における発明は、請求項１５から請求項２１のいずれか１項に記載のパラメータ変換装置において、前記エラー条件情報は、前記非負整数ｐ、前記非負整数ｑ、前記非負整数ｄ、前記非負整数ｄｆに対し、復号エラーが発生しないための条件を表す条件式２・ｐ・ｄ＋２・ｄｆ－１＜ｑ／２であることを特徴とする。

【００３９】

請求項２３における発明は、請求項１６から請求項２２のいずれか１項に記載のパラメータ変換装置において、前記出力パラメータ生成部は、１つ以上の格納格子強度係数と格納安全性決定情報の組を格納する格子強度係数格納手段を備え、前記格納格子強度係数と格納安全性決定情報は、外部から与えられることを特徴とする。

【００４０】

請求項２４における発明は、請求項２３に記載のパラメータ変換装置において、前記出力パラメータ生成部は、さらに、前記格子強度係数に基づいて前記格納安全性決定情報から、前記安全性決定情報を選択する安全性決定情報選択手段を備えることを特徴とする。

【００４１】

請求項２５における発明は、請求項２３に記載のパラメータ変換装置において

、前記出力パラメータ生成部は、前記格子強度係数と前記格納格子強度係数に基づいて前記仮パラメータ組を変更するか否かを判定する変更判定手段と、前記変更手段の判定に基づき、前記仮パラメータ組から変更仮パラメータ組を生成する仮パラメータ組変更手段を備え、前記安全性レベル情報に基づいて前記変更仮パラメータ組から前記出力パラメータを生成することを特徴とする。

【００４２】

請求項２６における発明は、請求項２５に記載のパラメータ変換装置において、前記仮パラメータ変更手段は、前記仮パラメータ組の前記非負整数ｄｇを変更して前記変更仮パラメータ組を生成することを特徴とする。

【００４３】

請求項２７における発明は、外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の暗号鍵と復号鍵を生成して出力する鍵生成装置と、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号装置と、前記暗号文を復号した復号文を生成して出力する復号装置とから構成される暗号化システムであって、前記パラメータ生成装置は、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵と前記復号鍵を生成し出力する生成鍵出力部を備え、前記暗号装置は、前記パラメータ生成装置が出力した出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備え、前記復号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする。

【００４４】

請求項２８における発明は、外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の暗号鍵を生成して出力する鍵生成装置と、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号装置とから構成される暗号化システムであって、前記パラメータ生成装置は、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵を生成し出力する生成鍵出力部を備え、前記暗号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備えることを特徴とする。

【００４５】

請求項２９における発明は、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して復号装置へ送信する暗号装置であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力する出力パラメータ生成部と、前記出力パラメータを前記復号装置へ送信するパラメータ送信部と、前記復号装置から前記出力パラメータに基づいて生成されたＮＴＲＵ暗号の暗号鍵を受信する暗号鍵受信部と、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して

前記暗号文を生成して送信する暗号文送信部を備えることを特徴とする。

【００４６】

請求項３０における発明は、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号化方法であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてＮＴＲＵ暗号の暗号鍵を生成するステップと、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを含むことを特徴とする。

【００４７】

請求項３１における発明は、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてＮＴＲＵ暗号の暗号鍵を生成するステップと、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを、コンピュータに実行させることを特徴とする。

【００４８】

請求項３２における発明は、外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の復号鍵を生成して出力する鍵生成装置と、外部から入

力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号装置とから構成される復号化システムであって、前記パラメータ生成装置は、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記復号鍵を生成し出力する生成鍵出力部を備え、前記復号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする。

【００４９】

請求項３３における発明は、暗号装置から受信した暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号装置であって、前記暗号装置から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを受信するパラメータ受信部と、前記出力パラメータを入力としてＮＴＲＵ暗号の暗号鍵と復号鍵を生成し出力する生成鍵出力部と、前記暗号鍵を前記暗号装置へ送信する暗号鍵送信部と、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して前記復号文を生成して出力する復号文生成部を備えることを特徴とする。

【００５０】

請求項３４における発明は、外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号化方法であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成

して出力するステップと、前記出力パラメータに基づいてＮＴＲＵ暗号の復号鍵を生成するステップと、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを含むことを特徴とする。

【００５１】

請求項３５における発明は、外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてＮＴＲＵ暗号の復号鍵を生成するステップと、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを、コンピュータに実行させることを特徴とする。

【００５２】

請求項３６における発明は、外部から入力された安全性レベル情報に基づき、外部から入力されたＮＴＲＵ暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータに変換して出力するパラメータ変換装置と、ＮＴＲＵ暗号の暗号鍵と復号鍵を生成して出力する鍵生成装置と、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号装置と、前記暗号文を復号した復号文を生成して出力する復号装置とから構成される暗号システムであって、前記パラメータ変換装置は、前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パ

ラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵と前記復号鍵を生成し出力する生成鍵出力部を備え、前記暗号装置は、前記パラメータ生成装置が出力した出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備え、前記復号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする。

【００５３】

請求項３７における発明は、外部から入力された安全性レベル情報に基づき、外部から入力されたＮＴＲＵ暗号のパラメータ組である入力パラメータと、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の暗号鍵を生成して出力する鍵生成装置と、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号装置とから構成される暗号化システムであって、前記パラメータ生成装置は、前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記暗号鍵を生成し出力する生成鍵出力部を備え、前記暗号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記暗号鍵を入力として、前記平文を暗号化して前記暗号文を生成して出力する暗号化部を備えることを特徴とする。

【００５４】

請求項３８における発明は、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して復号装置へ送信する暗号装置であって、予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発

生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力する出力パラメータ生成部と、前記出力パラメータを前記復号装置へ送信するパラメータ送信部と、前記復号装置から前記出力パラメータに基づいて生成されたＮＴＲＵ暗号の暗号鍵を受信する暗号鍵受信部と、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して前記暗号文を生成して送信する暗号文送信部を備えることを特徴とする。

【００５５】

請求項３９における発明は、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力する暗号化方法であって、予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてＮＴＲＵ暗号の暗号鍵を生成するステップと、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを含むことを特徴とする。

【００５６】

請求項４０における発明は、外部から入力された平文をＮＴＲＵ暗号で暗号化した暗号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えら

れた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてＮＴＲＵ暗号の暗号鍵を生成するステップと、前記出力パラメータと前記暗号鍵に基づいて、前記平文を暗号化して暗号文を生成して出力するステップとを、コンピュータに実行させることを特徴とする。

【００５７】

請求項４１における発明は、外部から入力された安全性レベル情報に基づき、外部から入力されたＮＴＲＵ暗号のパラメータ組である入力パラメータを、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置と、ＮＴＲＵ暗号の復号鍵を生成して出力する鍵生成装置と、外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号装置とから構成される復号化システムであって、前記パラメータ生成装置は、前記入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、前記仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、前記格子強度係数と前記安全性レベル情報に基づき、前記仮パラメータ組から前記出力パラメータを生成して出力する出力パラメータ生成部とを備え、前記鍵生成装置は、前記パラメータ生成装置が出力した前記出力パラメータを入力として前記復号鍵を生成し出力する生成鍵出力部を備え、前記復号装置は、前記パラメータ生成装置が出力した前記出力パラメータと前記鍵生成装置が出力した前記復号鍵を入力として、前記暗号文を復号して前記復号文を生成して出力する復号化部を備えることを特徴とする。

【００５８】

請求項４２における発明は、外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力する復号化方法であって、予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を

生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてＮＴＲＵ暗号の復号鍵を生成するステップと、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを含むことを特徴とする。

【００５９】

請求項４３における発明は、外部から入力された暗号文をＮＴＲＵ暗号で復号した復号文を生成して出力するプログラムを記録したコンピュータ読取可能な記録媒体であって、予め与えられたＮＴＲＵ暗号のパラメータ組である入力パラメータと予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成するステップと、前記仮パラメータ組から格子強度係数を計算するステップと、前記格子強度係数と予め与えられた安全性レベル情報に基づき、前記仮パラメータ組から、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するステップと、前記出力パラメータに基づいてＮＴＲＵ暗号の復号鍵を生成するステップと、前記出力パラメータと前記復号鍵に基づいて、前記暗号文を復号して復号文を生成して出力するステップとを、コンピュータに実行させることを特徴とする。

【００６０】

【発明の実施の形態】

以下、本発明に係るパラメータ生成装置及びパラメータ変換装置の実施の形態について、図面を用いて説明する。

【００６１】

本発明に係るパラメータ生成装置及びパラメータ変換装置は、ＮＴＲＵ暗号のパラメータを扱う。このＮＴＲＵ暗号については、非特許文献２に詳しく述べられているので、ここでは詳細な説明を省略するが、以下に簡単に説明する。

【００６２】

（１）ＮＴＲＵ暗号のパラメータ

ＮＴＲＵ暗号は、非負整数のパラメータ、Ｎ、ｐ、ｑ、ｄｆ、ｄｇ、ｄを持つ。非特許文献２には、ＮＴＲＵ暗号のパラメータの例として、（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）＝（１０７，３，６４，１５，１２，５）、（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）＝（１６７，３，１２８，６１，２０，１８）、（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）＝（５０３，３，２５６，２１６，７２，５５）の３つの例が挙げられている。

【００６３】

以下に、これらのパラメータの意味を説明する。

【００６４】

（ｉ）パラメータＮ

ＮＴＲＵ暗号は、多項式の演算により暗号化と復号化を行う公開鍵暗号方式である。ＮＴＲＵ暗号で扱う多項式の次元は、上記パラメータＮにより決まる。

【００６５】

ＮＴＲＵ暗号で扱う多項式は、上記パラメータＮに対し、Ｎ－１次元以下の整数係数多項式であり、例えばＮ＝５のとき、Ｘ＾４＋Ｘ＾３＋１等の多項式である。ここで、「Ｘ＾ａ」はＸのａ乗を意味することとする。また、暗号化時あるいは復号化時に用いる、公開鍵ｈ、秘密鍵ｆ、平文ｍ、乱数ｒ、暗号文ｃはいずれも、Ｎ－１次元以下の多項式として表現される（以降、それぞれを公開鍵多項式ｈ、秘密鍵多項式ｆ、平文多項式ｍ、乱数多項式ｒ、暗号文多項式ｃと呼ぶ）。

【００６６】

そして、多項式演算は、上記パラメータＮに対し、Ｘ＾Ｎ＝１という関係式を用いて、演算結果が常にＮ－１次元以下の多項式になるように演算される。例えば、Ｎ＝５の場合、多項式Ｘ＾４＋Ｘ＾２＋１と多項式Ｘ＾３＋Ｘの積は、多項式と多項式の積を×、整数と多項式の積（あるいは整数と整数の積）を・とすると、Ｘ＾５＝１という関係から、

（Ｘ＾４＋Ｘ＾２＋１）×（Ｘ＾３＋Ｘ）

＝Ｘ＾７＋２・Ｘ＾５＋２・Ｘ＾３＋Ｘ

＝Ｘ＾２×１＋２・１＋２・Ｘ＾３＋Ｘ

＝２・Ｘ＾３＋Ｘ＾２＋Ｘ＋２

というように、常にＮ－１次元以下の多項式になるように演算される。

【００６７】

（ｉｉ）パラメータｐ、ｑ

ＮＴＲＵ暗号では、非負整数のパラメータｐ、ｑを用いる。非特許文献２に記載の通り、このパラメータｐ、ｑは互いに素となる必要がある。

【００６８】

（ｉｉｉ）パラメータｄｆ、ｄｇ、ｄ

ＮＴＲＵ暗号で扱う秘密鍵多項式ｆ、公開鍵多項式を生成するときに秘密鍵多項式ｆと共に用いるランダム多項式ｇ、及び平文を暗号化するときに用いる乱数多項式ｒの選び方は、それぞれパラメータｄｆ、ｄｇ、ｄにより決まる。

【００６９】

まず、秘密鍵多項式ｆは、ｄｆ個の係数が１であり、かつ（ｄｆ－１）個の係数が－１であり、かつ他の係数は０となるように選ぶ。すなわち、乱数多項式ｆはＮ－１次元以下の多項式であり、０次元（定数項）からＮ－１次元まで、Ｎ個の係数があるが、このＮ個の係数のうち、ｄｆ個の係数が１であり、かつ（ｄｆ－１）個の係数が－１であり、かつ（Ｎ－２ｄｆ＋１）個の係数が０となるように選ぶ。

【００７０】

そして、ランダム多項式ｇは、ｄｇ個の係数が１であり、かつｄｇ個の係数が－１であり、かつ他の係数は０となるように選ぶ。また、乱数多項式ｒは、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつ他の係数は０となるように選ぶ。

【００７１】

（２）ＮＴＲＵ暗号の復号エラー

ところで、このＮＴＲＵ暗号は、平文多項式ｍを暗号化して暗号文多項式ｃを生成したとき、暗号文多項式ｃを復号して得られる復号文多項式ｍ’が平文多項式ｍと異なる場合が発生する。この場合は、復号時に正しく平文多項式ｍが得ら

れないことになる。このことを復号エラーが発生するという。

【００７２】

非特許文献２には、公開鍵多項式ｈの生成するときに用いるランダム多項式ｇ、乱数多項式ｒ、平文多項式ｍ、秘密鍵多項式ｆの演算結果の多項式（ｐ・ｒ×ｇ＋ｆ×ｍ）のいずれかの次数の係数の値が－ｑ／２からｑ／２の間に入らなかったとき、復号エラーが発生することが記載されている。非特許文献２に挙げられた上述の３つのパラメータにおいては、非特許文献５に記載の通り、小さい発生確率（１０＾（－５）程度）ではあるが復号エラーが発生してしまう。

【００７３】

（実施の形態１）

本発明に係る実施の形態１としてのパラメータ生成装置１について説明する。

【００７４】

＜パラメータ生成装置１の概要＞

最初に、図１を用いてパラメータ生成装置１の概要を説明する。

【００７５】

このパラメータ生成装置１は、あるパラメータのＮＴＲＵ暗号の格子強度係数ＧＬ、その格子強度係数ＧＬを持つＮＴＲＵ暗号の解読時間評価式ＥＦ、復号エラーが発生しないパラメータの条件式ＥＤ、及び初期安全性決定式ＩＦが予め与えられている。

【００７６】

そして、このパラメータ生成装置１は、外部より、ＮＴＲＵ暗号が達成すべき安全性レベルを示す安全性レベル情報ＳＬＩを入力したとき、予め与えられている、格子強度係数ＧＬと解読時間評価式ＥＦと条件式ＥＤと初期安全性決定式ＩＦを用いて、総当りの探索による解読とＬＬＬアルゴリズムによる解読に対し、入力された安全性レベル情報ＳＬＩが示す安全性レベルを達成し、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータ組ＰＳを生成して、外部へ出力する装置である。

【００７７】

以上が、パラメータ生成装置１の概要であるが、以下に、格子強度係数ＧＬ、

解読時間評価式ＥＦ、条件式ＥＤ、初期安全性決定式ＩＦの与え方について説明した後、パラメータ生成装置１の詳細について説明を行う。

【００７８】

＜格子強度係数ＧＬ、解読時間評価式ＥＦ、条件式ＥＤ＞

ここでは、まず、格子強度係数ＧＬ、解読時間評価式ＥＦ、復号エラーが発生しないパラメータの条件式ＥＤについてその内容を説明して、その与え方について説明する。

【００７９】

（格子強度係数ＧＬと解読時間評価式ＥＦ）

ＮＴＲＵ暗号における、ＬＬＬアルゴリズムを用いた解読時間Ｔの解読時間評価式ＥＦは、ＮＴＲＵ暗号のパラメータｄｆ、ｄｇ、ｑにより定まるものであって、パラメータｄｆ、ｄｇ、ｑから計算される格子強度係数ＧＬの値により類別される。非特許文献３には、格子強度係数ＧＬが、ＮＴＲＵ暗号のパラメータｄｆ、ｄｇ、ｑから、

ＧＬ＝（４・ｐｉ・ｅ・｜ｆ｜・｜ｇ｜／ｑ）＾（０．５）

のように導出されること、さらにその格子強度係数ＧＬが一定ならば、そのようなパラメータｄｆ、ｄｇ、ｑをもつＮＴＲＵ暗号に対しては、ある定数Ａ、Ｂが存在して、ＬＬＬアルゴリズムを用いた解読の解読時間ＴがパラメータＮに対し次の解読時間評価式ＥＦを満たすことが記載されている。

【００８０】

ＥＦ：ｌｏｇ（Ｔ）≧Ａ・Ｎ＋Ｂ

ここで、ｌｏｇ（Ｔ）は解読時間Ｔの自然対数である。また、ｐｉは円周率、ｅは自然対数の底、｜ｆ｜は秘密鍵多項式ｆのノルム、｜ｇ｜はランダム多項式のノルムを表す。具体的には、｜ｆ｜＝（２・ｄｆ－１）＾（０．５）、｜ｇ｜＝（２・ｄｇ）＾（０．５）である。

【００８１】

なお、非特許文献３には、上記に説明した解読時間評価式ＥＦにおける定数Ａ、Ｂについて、パラメータＮが小さいところでの解読時間Ｔを実測し、その実測データを用いて近似することによりその定数Ａ、Ｂの値を導けることが記載され

ている。

【００８２】

また、非特許文献４には、格子強度係数ＧＬの値が大きくなれば、ＬＬＬアルゴリズムを用いたＮＴＲＵ暗号の解読は、より難しくなることが記載されている。従って、いま、ある格子強度係数ＧＬ１の値に対し、格子強度係数ＧＬ１がその値をとるようなパラメータｄｆ、ｄｇ、ｑをもつＮＴＲＵ暗号に対する、ＬＬＬアルゴリズムを用いた解読の解読時間Ｔの解読時間評価式ＥＦ１が、

ＥＦ１：ｌｏｇ（Ｔ）≧Ａ・Ｎ＋Ｂ　（Ａ、Ｂ：定数）

で与えられているとする。すると、以上の議論により、別のパラメータｄｆ、ｄｇ、ｑから導出される格子強度係数ＧＬの値が、もし、上記の格子強度係数ＧＬ１の値よりも大きければ、その別のパラメータｄｆ、ｄｇ、ｑをもつＮＴＲＵ暗号の解読時間Ｔは、少なくとも上記の解読時間評価式ＥＦ１を満たすことが導ける。

【００８３】

（復号エラーが発生しないパラメータの条件式ＥＤ）

非特許文献２には、ＮＴＲＵ暗号の復号プロセスにおいて計算される多項式、ｐ・ｒ×ｇ＋ｆ×ｍの全ての係数が、－ｑ／２からｑ／２の範囲に収まっていれば、正しく復号処理を行うことができ、復号エラーが発生しないことが記載されている。

【００８４】

（格子強度係数ＧＬと解読時間評価式ＥＦの与え方）

まず、パラメータｄｆ、ｄｇ、ｑの値を決定する。ここでは、一例として、ｄｆ＝３４、ｄｇ＝３４、ｑ＝５１２とする。そして、このパラメータｄｆ、ｄｇ、ｑから上記格子強度係数ＧＬの値を計算し、その格子強度係数ＧＬを、予め式格納部１１０に与えておく。上記例では、格子強度係数ＧＬはＧＬ＝２．１２となる。

【００８５】

次に、解読時間評価式ＥＦとして、上記格子強度係数ＧＬの値に対し、その値をとるパラメータｄｆ、ｄｇ、ｑをもつＮＴＲＵ暗号の解読時間Ｔの解読時間評

価式ＥＦを、以下のようにして求め、予め式格納部１１０に与えておく。

【００８６】

すなわち、上記解読時間評価式ＥＦは、パラメータｄｆ、ｄｇ、ｑから計算される格子強度係数の値が２．１２以上であるときに、ＬＬＬアルゴリズムを用いた解読の解読時間Ｔを、少なく見積もることなく評価できるものである。

【００８７】

（ｉ）パラメータＮが小さいところでの解読時間Ｔを導出

まず、決定したパラメータｄｆ、ｄｇ、ｑに対し、非特許文献３に記載の方法で、ＬＬＬアルゴリズムを用いた場合の解読時間Ｔの実測データを実験により求める。ここで、図２に示す解読時間Ｔの実測データは、１０００ＭＩＰＳの処理能力をもつコンピュータを用いて求めたものであり、解読時間Ｔの単位は秒である。なお、ＭＩＰＳ（Ｍｉｌｌｉｏｎ　Ｉｎｓｔｒｕｃｔｉｏｎ　Ｐｅｒ　Ｓｅｃｏｎｄ）とは、コンピュータの処理能力を表す単位であり、１ＭＩＰＳとは、１秒間に１００万命令を実行できる処理能力を表す。本例ではパラメータＮとして７０から９０までの値に対して解読時間が実測可能であったことを示している。

【００８８】

（ｉｉ）近似による解読時間評価式の導出

次に、（ｉ）により導出した実測データを用い、解読時間評価式ＥＦ

ＥＦ：ｌｏｇ（Ｔ）＝Ａ・Ｎ＋Ｂ

の定数Ａ、Ｂを求める。これは、例えば、Ｘ＝Ｎ、Ｙ＝ｌｏｇ（Ｔ）として、Ｙ＝Ａ・Ｘ＋Ｂの係数Ａ、Ｂを最小二乗法により求めれば実現できる。

【００８９】

ここで、図２に示す解読時間Ｔの実測データの場合、定数Ａ、Ｂは、概ね、Ａ＝０．０９３、Ｂ＝－３．８となる。

【００９０】

基本的には、これにより導出された解読時間評価式ＥＦ

ＥＦ：ｌｏｇ（Ｔ）＝０．０９３Ｎ－３．８

を式格納部１１０に与えてもよいが、以下に詳細を述べる実施の形態１では、解

読時間評価式ＥＦにおける解読時間Ｔの値を、ＭＩＰＳｙｅａｒ値として扱っている。なお、ＭＩＰＳｙｅａｒとはコンピュータの処理量を示す単位であり、１ＭＩＰＳの処理能力を持つコンピュータが１年間で処理できる処理量が１ＭＩＰＳｙｅａｒである。

【００９１】

従って、ここでは、導出された解読時間評価式ＥＦを、非特許文献３に記載の方法で、解読時間Ｔに、実測データを求めたコンピュータの処理能力値１０００ＭＩＰＳを乗じ、１年間の秒数３１５５７６００（１年間＝３６５．２５日）で割って、解読時間ＴがＭＩＰＳｙｅａｒ値を表すように変形する。

【００９２】

すなわち、Ｔ’＝１０００Ｔ／３１５５７６００とし、前述の解読時間評価式ＥＦに代入することにより、次のように変形した解読時間評価式ＥＦを式格納部１１０に与える。

【００９３】

ＥＦ：ｌｏｇ（Ｔ’）＝０．０９３Ｎ－１４．２

なお、最小二乗法についてはよく知られた公知の方法であるので、ここでは説明を省略する。

【００９４】

（復号エラーが発生しないパラメータの条件式ＥＤの与え方）

次に、条件式ＥＤの与え方について述べる。

【００９５】

まず、ｐ＝３とし、ｄｇ＞ｄとする。これは、ＮＴＲＵ暗号のパラメータの典型的な値である。

【００９６】

このとき、条件式ＥＤ

ＥＤ：６ｄ＋２ｄｆ－１＜ｑ／２

を予め式格納部１１０に与えておく。この条件式は、理論的に復号エラーが発生しないパラメータの条件式である。

【００９７】

以下に、その理由について説明する。

【００９８】

まず、上述したように、多項式ｐ・ｒ×ｇ＋ｆ×ｍの全ての係数が、－ｑ／２からｑ／２の範囲に収まっていれば、復号エラーは発生しない。

【００９９】

このとき、多項式ｒ×ｇを考えると、多項式の積は、非特許文献２に記載の通り、多項式ａのｋ次の係数をａ（ｋ）で表すと、

（ｒ×ｇ）（ｋ）

＝ｒ（０）・ｇ（ｋ）＋ｒ（１）・ｇ（ｋ－１）＋．．．

＋ｒ（Ｎ－１）・ｇ（ｋ－（Ｎ－１）（ｍｏｄ　Ｎ））

である。そして、乱数多項式ｒは、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつ他の係数は０となる多項式である。そして、ランダム多項式ｇは、ｄｇ個の係数が１であり、かつｄｇ個の係数が－１であり、かつ他の係数は０となる多項式である。

【０１００】

従って、多項式ｒ×ｇのｋ次の係数（ｒ×ｇ）（ｋ）の値は、ｄｇ＞ｄであるので、

（ｒ×ｇ）（ｋ）

＝１・ｇ（ｉ１）＋１・ｇ（ｉ２）＋．．．＋１・ｇ（ｉｄ）

－１・ｇ（ｊ１）－１・ｇ（ｊ２）－．．．－１・ｇ（ｊｄ）

というように、ｄ個の１・ｇ（ｉｎ）という項（１≦ｎ≦ｄ）とｄ個の－１・ｇ（ｊｎ）という項（１≦ｎ≦ｄ）で表される。

【０１０１】

よって、（ｒ×ｇ）（ｋ）は、ｇ（ｉｎ）が全て１であり（１≦ｎ≦ｄ）、かつｇ（ｊｎ）が全て－１であるようなとき（１≦ｎ≦ｄ）最大値を取り、その値は、高々２ｄである（最小値も、せいぜい－２ｄである。）。

【０１０２】

同様に、多項式ｆ×ｍのｋ次の係数の値も、その値は高々２ｄｆ－１である（最小値も、せいぜい－２ｄｆ＋１である。）。

【０１０３】

今、ｐ＝３であるので、以上により、多項式ｐ・ｒ×ｇ＋ｆ×ｍの最も大きい係数の値は、高々３・２ｄ＋２ｄｆ－１である。そして、最も大きい係数がｑ／２を超えなければ、多項式ｐ・ｒ×ｇ＋ｆ×ｍの全ての係数は、－ｑ／２からｑ／２の範囲に収まっていることになるので、復号エラーは発生しない。

【０１０４】

従って、以下の条件式ＥＤが導かれる。

【０１０５】

ＥＤ：６ｄ＋２ｄｆ－１＜ｑ／２

この条件式を満たせば、以上の議論から復号エラーは理論的に発生しない。

【０１０６】

＜初期安全性決定式ＩＦ＞

詳細は後述するが、パラメータ生成装置１は、まず、総当り探索の解読に対し安全であるパラメータｄｆ、ｄｇ、ｄを選ぶために、第１のパラメータ生成部１０２において、安全性レベル情報ＳＬＩに応じた十分大きい値であるパラメータＮを選ぶ必要がある。

【０１０７】

ここでは、そのために、初期安全性決定式ＩＦの一例として、非特許文献３に挙げられている、パラメータｄｆ、ｄｇ、ｑが、ｄｆ＝６１、ｄｇ＝２０、ｑ＝１２８の場合のＮＴＲＵ暗号における、ＬＬＬアルゴリズムによる解読に必要な解読時間の評価式とし、

ＩＦ：ｌｏｇ（Ｔ）＝０．２００２Ｎ－１８．８８４

とする。そして、この初期安全性決定式ＩＦを、式格納部１１０へ与えておく。

【０１０８】

パラメータｄｆ、ｄｇ、ｑが、ｄｆ＝６１、ｄｇ＝２０、ｑ＝１２８の場合のＮＴＲＵ暗号における、ＬＬＬアルゴリズムによる解読に必要な解読時間の評価式である、ｌｏｇ（Ｔ）＝０．２００２Ｎ－７．６０８という式を、ＴがＭＩＰＳｙｅａｒを表すように変換した式である。

【０１０９】

次に、パラメータ生成装置１の詳細について説明を行う。

【０１１０】

＜パラメータ生成装置１の構成＞

パラメータ生成装置１は、図１に示すように、入力部１０１と、第１のパラメータ生成部１０２と、第２のパラメータ生成部１０３と、第３のパラメータ生成部１０４と、安全性判定部１０５と、安全性増加部１０６と、出力部１０７と、第１のパラメータ変更部１０８と、第２のパラメータ変更部１０９と、式格納部１１０から構成される。以下にそれぞれの構成要素について説明する。

【０１１１】

（１）入力部１０１

入力部１０１は、外部から安全性レベル情報ＳＬＩを受け取り、安全性レベル情報ＳＬＩを第１のパラメータ生成部１０２と第２のパラメータ生成部１０３と安全性増加部１０６と第２のパラメータ変更部１０９に出力する。

【０１１２】

ここで、安全性レベル情報ＳＬＩとは、達成すべき暗号の安全性レベルを表す情報であり、例えば、暗号の安全性が１０２４ビットＲＳＡ暗号に相当する安全性レベルであることを示す情報である。ここでは、一例として、安全性レベル情報ＳＬＩは、暗号解読アルゴリズムの処理量とする。ここでは、ＳＬＩは（１０＾１２）ＭＩＰＳｙｅａｒであるとして以降の説明を行う。

【０１１３】

（２）第１のパラメータ生成部１０２

第１のパラメータ生成部１０２は、入力部１０１から安全性レベル情報ＳＬＩを受け取り、式格納部１１０から初期安全性決定式ＩＦを読み取り、安全性レベル情報ＳＬＩに応じた十分大きい値である、ＮＴＲＵ暗号のパラメータＮを選ぶ。そして、選んだパラメータＮに対し、パラメータｐ＝３とし、その他のパラメータｑ、ｄｆ、ｄｇ、ｄの値を仮に０として、パラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して第２のパラメータ生成部１０３へ出力する。

【０１１４】

具体的には、パラメータＮは、初期安全性決定式ＩＦの値が安全性レベル情報

ＳＬＩの表す安全性レベルとなるようにパラメータＮを選ぶ。

【０１１５】

例えば、安全性レベル情報ＳＬＩが（１０＾１２）ＭＩＰＳｙｅａｒであり、式格納部１１０に格納されている初期安全性決定式ＩＦが

ＩＦ：ｌｏｇ（Ｔ）＝０．２００２Ｎ－１８．８８４

であるとき、安全性レベル情報ＳＬＩをＴに代入した結果

ＩＦ：ｌｏｇ（１０＾１２）＝０．２００２Ｎ－１８．８８４

を計算することにより、Ｎ＝２３３を導出する。

【０１１６】

（３）第２のパラメータ生成部１０３

第２のパラメータ生成部１０３は、第１のパラメータ生成部１０２もしくは第１のパラメータ変更部１０８からパラメータ組ＰＳを受け取り、入力部１０１から安全性レベル情報ＳＬＩを受け取る。そして、パラメータ組ＰＳの中のパラメータＮに基づき後述する方法によりパラメータ候補集合ＤＳを導出する。そして、後述する方法によりＤＳの要素数がパラメータｄｆ、ｄｇ、ｄを選ぶのに不十分かどうか（例えば、要素数が３以上かどうか）を判別する。不十分であれば、パラメータ組ＰＳを第１のパラメータ変更部１０８へ出力する。十分であれば、第２のパラメータ生成部１０３はパラメータｄｆ、ｄｇ、ｄを、パラメータ候補集合ＤＳから選択し、これらのパラメータｄｆ、ｄｇ、ｄに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して第３パラメータ生成部１０４へ出力する。

【０１１７】

以下に、パラメータ候補集合ＤＳの導出方法と、パラメータｄｆ、ｄｇ、ｄの選択方法について詳細に説明する。

【０１１８】

（ｉ）パラメータ候補集合ＤＳの導出方法

安全性レベル情報ＳＬＩとパラメータＮに対し、

（Ｃ（Ｎ，ｋ）・Ｃ（Ｎ－ｋ，ｋ））＾（０．５）≧ＳＬＩ

を満たす整数ｋ（１≦ｋ≦Ｎ）のパラメータ候補集合ＤＳを導出する。ここで、

Ｃ（ａ，ｂ）はａ個の中からｂ個を選ぶ組み合わせの数である。

【０１１９】

これは、例えば、パラメータＮに対し、ｋ＝１からｋ＝Ｎ／２まで順に上記の左辺を計算して右辺の安全性レベル情報ＳＬＩと比較し、左辺の値が右辺の安全性レベル情報ＳＬＩ以上の値となるそれぞれのｋを、パラメータ候補集合ＤＳの要素とすることで実現できる。

【０１２０】

なお、上記の式の左辺は、ｄｇ＝ｋ（もしくはｄｆ＝ｋ）としたときには、非特許文献５に記載の通り、ＮＴＲＵ暗号の秘密鍵を総当りで探索する暗号解読の解読時間を示し、ｄ＝ｋとしたときには、非特許文献５に記載の通り、ＮＴＲＵ暗号の平文を総当りで探索する暗号解読の解読時間を示す。すなわち、ここでは、パラメータ候補集合ＤＳの中からパラメータｄｆ、ｄｇ、ｄを選べば、平文や秘密鍵を総当りで探索する解読の解読時間が入力部１０１に入力された安全性レベル情報ＳＬＩが表す安全性レベルを達成するように、パラメータ候補集合ＤＳを導出している。

【０１２１】

（ｉｉ）パラメータｄｆ、ｄｇ、ｄの選択方法

パラメータｄｆ、ｄｇ、ｄは、ｄｇ＞ｄとなるように、パラメータ候補集合ＤＳから任意に選択する。ここでは、ｄｆ＞ｄｇ＞ｄとなるように、パラメータ候補集合ＤＳからランダムに選択してそれぞれｄｆ、ｄｇ、ｄに割り当てることとする。

【０１２２】

なお、パラメータ候補集合ＤＳは、十分大きいＮに対しては、その要素数がパラメータｄｆ、ｄｇ、ｄを選ぶのに十分な数となる。実際に、ＳＬＩ＝１０＾１２とすると、Ｎ＝１０のときにはＤＳの要素は無いが、Ｎ＝３０のときにはＤＳ＝｛８，９，１０，１１，１２｝（８以上１２以下の５個の整数）となり、Ｎ＝１００のときにはＤＳ＝｛４，５，６，．．．，５０｝（４以上５０以下の４７個の整数）となる。

【０１２３】

（４）第３のパラメータ生成部１０４

第３のパラメータ生成部１０４は、第２のパラメータ生成部１０３からパラメータ組ＰＳを受け取り、式格納部１１０から復号エラーが発生しないためのパラメータの条件式ＥＤを読み取る。そして、パラメータ組ＰＳの中のパラメータｄｆ、ｄｇ、ｄに対し、条件式ＥＤを満たし、かつ、パラメータｑが２の冪となるような最小のｑをパラメータｑとして選ぶ。そして、選んだパラメータｑに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して安全性判定部１０５へ出力する。

【０１２４】

例えば、ｄｆ＝５０、ｄｇ＝２４、ｄ＝１６で、条件式ＥＤが

ＥＤ：６ｄ＋２ｄｆ－１＜（ｑ／２）

のとき、この条件式を解くとｑ＞２９４となり、この条件式を満たしかつｑ＝２＾ｉ（ｉは自然数）を満たす最小のｑは５１２であるので、パラメータｑをｑ＝５１２とする。なお、パラメータｑを２の冪とするのは、パラメータｐ（ｐ＝３）とパラメータｑを互いに素になるように選ぶためである。ｐとｑが互いに素になることは、非特許文献２に記載の通り、ＮＴＲＵ暗号のパラメータｐ、ｑの条件である。

【０１２５】

（５）安全性判定部１０５

安全性判定部１０５は、第３のパラメータ生成部１０４もしくは第２のパラメータ変更部１０９からパラメータ組ＰＳを受け取り、パラメータ組ＰＳの中のパラメータＮ、ｐ、ｑ、ｄｆ、ｄｇを持つＮＴＲＵ暗号の格子強度係数ＳＬを、パラメータｄｆ、ｄｇ、ｑを用いて

ＳＬ＝（４・ｐｉ・ｅ・｜ｆ｜・｜ｇ｜／ｑ）＾（０．５）

により導出する。ここで、ｐｉは円周率、ｅは自然対数の底、｜ｆ｜＝（２ｄｆ－１）＾（０．５）、｜ｇ｜＝（２ｄｇ）＾（０．５）を表す。

【０１２６】

そして、安全性判定部１０５は、式格納部１１０から格子強度係数ＧＬを読み取り、ＧＬ≦ＳＬならば、パラメータ組ＰＳを安全性増加部１０６へ出力する。

そうでなければ、パラメータ組ＰＳを第２のパラメータ変更部１０９へ出力する。

【０１２７】

（６）安全性増加部１０６

安全性増加部１０６は、安全性判定部１０５からパラメータ組ＰＳを受け取り、入力部１０１から安全性レベル情報ＳＬＩを受け取り、式格納部１１０より解読時間評価式ＥＦを読み取る。そして、パラメータ組ＰＳの中のパラメータＮと解読時間評価式ＥＦからＮＴＲＵ暗号の解読時間Ｔを導出する。

【０１２８】

例えば、Ｎ＝４００、解読時間評価式ＥＦが、

ＥＦ：ｌｏｇ（Ｔ）＝０．０９３Ｎ－１４．２

であるとき、Ｔはおよそ９．７×１０＾９である。

【０１２９】

そして、安全性増加部１０６は、導出した解読時間Ｔが、安全性レベル情報ＳＬＩが表す安全性レベルを達成しているかどうかを

Ｔ≧ＳＬＩ

を満たすかどうかによって判定する。そして、Ｔ＜ＳＬＩならば、解読時間Ｔが、Ｔ≧ＳＬＩとなるようにパラメータＮを増加させ、増加させたパラメータＮに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成する。

【０１３０】

これは、例えば、安全性レベル情報ＳＬＩを解読時間評価式ＥＦのＴに代入した結果

ＥＦ：ｌｏｇ（ＳＬＩ）＝０．０４０Ｎ－６．２

を計算してＮを導出し、パラメータ組ＰＳを生成すればよい。

【０１３１】

そして、安全性増加部１０６は、パラメータ組ＰＳの中のパラメータＮに対し、パラメータＮが素数かどうかを判定する。そして、パラメータＮが素数でないならば、パラメータＮを増加させて素数となるようにして、増加させたパラメータＮに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成

する。

【０１３２】

例えば、ＰＳ＝（４５０，３，５１２，５０，２４，１６）の場合、パラメータＮはＮ＝４５０であるが素数ではないので、４５０を超える素数のうち最小のものである４５１を新たにパラメータＮの値として、ＰＳ＝（４５１，３，５１２，５０，２４，１６）とする。

【０１３３】

これは、パラメータＮが合成数だと、ＮＴＲＵ暗号の安全性が低下することが知られているため、これを避ける目的で行われるものである。なお、素数かどうかを判定する方法は、例えば、非特許文献１に記載されており、ここでの説明は省略する。

【０１３４】

そして、安全性増加部１０６は、パラメータ組ＰＳを出力部１０７へ出力する。

【０１３５】

（７）出力部１０７

出力部１０７は、安全性増加部１０６からパラメータ組ＰＳを受け取って外部へ出力する。

【０１３６】

（８）第１のパラメータ変更部１０８

第１のパラメータ変更部１０８は、第２のパラメータ生成部１０３もしくは第２のパラメータ変更部１０９からパラメータ組ＰＳを受け取り、パラメータ組ＰＳの中のパラメータＮを増加させる。ここでは、一例として、Ｎを１０増加させるとする。そして、増加させたパラメータＮに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して第２のパラメータ生成部１０３へ出力する。

【０１３７】

（９）第２のパラメータ変更部１０９

第２のパラメータ変更部１０９は、入力部１０１から安全性レベル情報ＳＬＩ

を受け取り、安全性判定部１０５からパラメータ組ＰＳを受け取り、そして、第２のパラメータ生成部１０３と同様にして、パラメータ候補集合ＤＳを生成する。そして、パラメータ組ＰＳの中のパラメータｄｇとパラメータ候補集合ＤＳの要素の最大値Ｍを比較し、ｄｇ＜Ｍであれば、パラメータｄｇを、パラメータ候補集合ＤＳの要素のうち、より大きい値に変更し、変更したパラメータｄｇに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して安全性判定部１０５へ出力する。そうでなければ、パラメータ組ＰＳを第１パラメータ変更部１０８へ出力する。

【０１３８】

（１０）式格納部１１０

式格納部１１０は、図３に示すように、予め、格子強度係数ＧＬ、解読時間評価式ＥＦ、復号エラーが発生しないパラメータの条件式ＥＤ、及び初期安全性決定式ＩＦが与えられている。ここでは、前述のとおり、格子強度係数ＧＬは、

ＧＬ＝２．１２，

解読時間評価式ＥＦは、

ＥＦ：ｌｏｇ（Ｔ）＝０．９３Ｎ－１４．２，

条件式ＥＤは、

ＥＤ：６ｄ＋２ｄｆ－１＜（ｑ／２），

初期安全性決定式ＩＦは、

ＩＦ：ｌｏｇ（Ｔ）＝０．２００２Ｎ－１８．８８４

が、予め与えられているとする。

【０１３９】

ここで、上記解読時間評価式ＥＦは、前述したとおり、パラメータｄｆ、ｄｇ、ｑから計算される格子強度係数の値が、上記格子強度係数ＧＬの値以上であるとき（この場合は２．１２以上であるとき）に、ＬＬＬアルゴリズムを用いた解読の解読時間Ｔを、少なく見積もることなく評価できるものである。

【０１４０】

また、条件式ＥＤは、前述したとおり、ＮＴＲＵ暗号において、復号エラーが発生しないためのパラメータ条件を表す式であり、初期安全性決定式ＩＦは、ま

ず、総当り探索の解読に対し安全であるパラメータｄｆ、ｄｇ、ｄを選ぶために、第１のパラメータ生成部１０２において、安全性レベル情報ＳＬＩに応じた十分大きい値であるパラメータＮを選ぶために用いられる式である。

【０１４１】

＜パラメータ生成装置１の動作＞

以上に述べたパラメータ生成装置１の動作について、図４、図５に示すフローチャートを用いて説明する。

【０１４２】

パラメータ生成装置１は、あるパラメータのＮＴＲＵ暗号の格子強度係数ＧＬ、その格子強度係数ＧＬを持つＮＴＲＵ暗号の解読時間評価式ＥＦ、及び復号エラーが発生しないパラメータの条件式ＥＤが予め与えられており、外部より安全性レベル情報ＳＬＩが入力されると、以下の処理を行う。

【０１４３】

最初に、入力部１０１は、外部から安全性レベル情報ＳＬＩを受け取り、安全性レベル情報ＳＬＩを第１のパラメータ生成部１０２と第２のパラメータ生成部１０３と安全性増加部１０６に出力する（ステップＳ１０１）。

【０１４４】

次に、第１のパラメータ生成部１０２は、入力部１０１から安全性レベル情報ＳＬＩを受け取り、式格納部１１０から初期安全性決定式ＩＦを読み取り、安全性レベル情報ＳＬＩに応じた十分大きい値である、ＮＴＲＵ暗号のパラメータＮを選ぶ（ステップＳ１０２）。

【０１４５】

そして、第１のパラメータ生成部１０２は、選んだパラメータＮに対し、パラメータｐ＝３とし、その他のパラメータｑ、ｄｆ、ｄｇ、ｄの値を仮に０として、パラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して第２のパラメータ生成部１０３へ出力する（ステップＳ１０３）。

【０１４６】

次に、第２のパラメータ生成部１０３は、第１のパラメータ生成部１０２もしくは第１のパラメータ変更部１０８からパラメータ組ＰＳを受け取り、入力部１

０１から安全性レベル情報ＳＬＩを受け取る（ステップＳ１０４）。

【０１４７】

そして、第２のパラメータ生成部１０３は、パラメータ候補集合ＤＳを生成する（ステップＳ１０５）。

【０１４８】

そして、第２のパラメータ生成部１０３は、ＤＳの要素数がパラメータｄｆ、ｄｇ、ｄを選ぶのに不十分かどうかを判別し、不十分だったら、処理をステップＳ１０７へ移す。そうでなければステップＳ１０９へ処理を移す（ステップＳ１０６）。

【０１４９】

そして、第２のパラメータ生成部１０３は、パラメータ組ＰＳを第１パラメータ変更部１０８へ出力する。（ステップＳ１０７）。

【０１５０】

次に、第１のパラメータ変更部１０８は、第２のパラメータ生成部１０３もしくは第２のパラメータ変更部１０９からパラメータ組ＰＳを受け取り、パラメータ組ＰＳの中のパラメータＮを増加させ、増加させたパラメータＮに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して第２のパラメータ生成部１０３へ出力する。そして、処理をステップＳ１０４へ移す（ステップＳ１０８）。

【０１５１】

そして、第２のパラメータ生成部１０３は、パラメータ候補集合ＤＳの要素からパラメータｄｆ、ｄｇ、ｄを選び、選んだパラメータｄｆ、ｄｇ、ｄに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して第３パラメータ生成部１０４へ出力する（ステップＳ１０９）。

【０１５２】

次に、第３のパラメータ生成部１０４は、第２のパラメータ生成部１０３からパラメータ組ＰＳを受け取り、式格納部１１０から復号エラーが発生しないパラメータの条件式ＥＤを読み取る（ステップＳ１１０）。

【０１５３】

そして、第３のパラメータ生成部１０４は、パラメータ組ＰＳの中のパラメータｄｆ、ｄｇ、ｄに対し、条件式ＥＤを満たし、かつ、パラメータｑが２の冪となるような最小のｑをパラメータｑとして選び、選んだパラメータｑに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して安全性判定部１０５へ出力する（ステップＳ１１１）。

【０１５４】

次に、安全性判定部１０５は、第３のパラメータ生成部１０４もしくは第２のパラメータ変更部１０９からパラメータ組ＰＳを受け取り、パラメータ組ＰＳの中のパラメータＮ、ｐ、ｑ、ｄｆ、ｄｇをもつＮＴＲＵ暗号の格子強度係数ＳＬを導出する（ステップＳ１１２）。

【０１５５】

そして、安全性判定部１０５は、式格納部１１０から格子強度係数ＧＬを読み取り、ＧＬ≦ＳＬならば、ステップＳ１１４へ処理を移す。そうでなければ、ステップＳ１２３へ処理を移す（ステップＳ１１３）。

【０１５６】

そして、安全性判定部１０５は、パラメータ組ＰＳを安全性増加部１０６へ出力する（ステップＳ１１４）。

【０１５７】

次に、安全性増加部１０６は、安全性判定部１０５からパラメータ組ＰＳを受け取り、入力部１０１から安全性レベル情報ＳＬＩを受け取り、式格納部１１０より解読時間評価式ＥＦを読み取る（ステップＳ１１５）。

【０１５８】

そして、安全性増加部１０６は、パラメータ組ＰＳの中のパラメータＮと解読時間評価式ＥＦからＮＴＲＵ暗号の解読時間Ｔを導出する（ステップＳ１１６）。

【０１５９】

そして、安全性増加部１０６は、導出した解読時間Ｔが、Ｔ＜ＳＬＩならば、ステップＳ１１８へ処理を移す。そうでなければ、ステップＳ１１９へ処理を移す（ステップＳ１１７）。

【０１６０】

そして、安全性増加部１０６は、解読時間ＴがＴ≧ＳＬＩとなるようにパラメータＮを増加させ、増加させたパラメータＮに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成する（ステップＳ１１８）。

【０１６１】

そして、安全性増加部１０６は、パラメータＮが素数であれば、ステップＳ１２１へ処理を移す。そうでなければステップＳ１２０へ処理を移す（ステップＳ１１９）。

【０１６２】

そして、安全性増加部１０６は、パラメータＮを増加させ、増加させたパラメータＮが素数となるようにし、増加させたパラメータＮに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成する（ステップＳ１２０）。

【０１６３】

そして、安全性増加部１０６は、パラメータ組ＰＳを出力部１０７へ出力する（ステップＳ１２１）。

【０１６４】

次に、出力部１０７は、安全性増加部１０６からパラメータ組ＰＳを受け取り、パラメータ組ＰＳを外部へ出力して処理を終了する（ステップＳ１２２）。

【０１６５】

次に、第２のパラメータ変更部１０９は、入力部１０１から安全性レベル情報ＳＬＩを受け取り、安全性判定部１０５からパラメータ組ＰＳを受け取り、パラメータ候補集合ＤＳを生成する（ステップＳ１２３）。

【０１６６】

そして、第２のパラメータ変更部１０９は、パラメータ組ＰＳの中のパラメータｄｇとパラメータ候補集合ＤＳの要素の最大値Ｍを比較し、ｄｇ＜Ｍであれば、処理をステップＳ１２５へ移す。そうでなければ、ステップＳ１２６へ処理を移す（ステップＳ１２４）。

【０１６７】

そして、第２のパラメータ変更部１０９は、パラメータｄｇを、パラメータ候

補集合ＤＳの要素のうち、より大きい値に変更し、変更したパラメータｄｇに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成し、パラメータ組ＰＳを安全性判定部１０５へ出力して、処理をステップＳ１１２へ移す（ステップＳ１２５）。

【０１６８】

そして、第２のパラメータ変更部１０９は、パラメータ組ＰＳを第１のパラメータ変更部１０８へ出力して、処理をステップＳ１０８へ移す（ステップＳ１２６）。

【０１６９】

＜パラメータ生成装置１の動作検証＞

以下に、実施の形態１におけるパラメータ生成装置１の全体の動作について説明する。

【０１７０】

まず、第１のパラメータ生成部１０２が、ステップＳ１０２において、安全性レベル情報ＳＬＩに応じた十分大きい値である、パラメータＮを選んでいる。

【０１７１】

そして、第２のパラメータ生成部１０３が、ステップＳ１０６において、ＮＴＲＵ暗号を総当りで探索する解読に対し、安全性レベル情報ＳＬＩの表す安全性レベルを達成するパラメータ候補集合ＤＳを生成して、ステップＳ１０９において、このパラメータ候補集合ＤＳの要素から、安全性レベル情報ＳＬＩの表す安全性レベルを達成するパラメータｄｆ、ｄｇ、ｄを選んでいる。

【０１７２】

なお、パラメータ候補集合ＤＳの要素数が不十分な場合は、第１のパラメータ変更部１０８が、ステップＳ１０８において、パラメータＮを増加させるようにしている。上述したように、一般に、パラメータＮが増加すれば、パラメータ候補集合ＤＳの要素数も大きくなるので、必ずパラメータｄｆ、ｄｇ、ｄは選ぶことができる。

【０１７３】

そして、第３のパラメータ生成部１０４が、ステップＳ１１１において、復号

エラーが発生しないパラメータの条件式ＥＤを満たすように、パラメータｑを選ぶことにより、パラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）の値が決まる。

【０１７４】

ここで、パラメータｑの値は、条件式ＥＤを満たすように選ぶと、同程度のパラメータｄｆ、ｄｇ、ｄをもつ、非特許文献２や非特許文献３に記載のＮＴＲＵ暗号におけるパラメータｑに比べ、一般に大きくなる。すなわち、格子強度係数ＧＬの値が小さくなるので、同程度のパラメータｄｆ、ｄｇ、ｄをもつ非特許文献２や非特許文献３に記載のＮＴＲＵ暗号に比べ、ＬＬＬアルゴリズムによる解読に対する安全性レベル（解読時間）が下がる可能性がある。

【０１７５】

従って、予め格納されている格子強度係数ＧＬに基づき、安全性判定部１０５が、ステップＳ１１３において、生成されたパラメータ組ＰＳをもつＮＴＲＵ暗号の解読時間が、その格子強度係数ＧＬに基づく解読時間評価式ＥＦで評価可能かどうかを判断し、そして、評価可能であれば、安全性増加部１０６が、ステップＳ１１８において、安全性レベル情報ＳＬＩの表す安全性レベルを達成するようにパラメータＮを増加させている。

【０１７６】

なお、そうでない場合には、第２のパラメータ変更部１０９が、ステップＳ１２５において、パラメータｄｇをより大きい値にすることにより、そのパラメータをもつＮＴＲＵ暗号の格子強度係数の値を大きくして、解読時間評価式ＥＦで評価できるようにするか、それで対応できない場合は、第１のパラメータ変更部１０８が、ステップＳ１０８で、パラメータＮを増加させ、そしてステップＳ１０９以降で、もう一度パラメータｄｆ、ｄｇ、ｄ、ｑの生成を行うようにしている。

【０１７７】

今、パラメータＮを大きくとれば、一般にパラメータ候補集合ＤＳは大きい要素をもつようになる。よって、ステップＳ１０９で、パラメータｄｆ、ｄｇ、ｄをもう一度選び直すときには、ｄｆ、ｄの値を変えずに、ｄｇのみ値を大きくと

ることができる。そして、ｄｇの値は、復号エラー発生の条件式には関与しないので、復号エラーが発生しないことを保証したまま、格子強度係数ＧＬの値を大きくして、解読時間評価式ＥＦで評価できるようにすることが可能となる。

【０１７８】

以上により、高々有限回の繰り返し回数で、総当りの探索による解読とＬＬＬアルゴリズムによる解読に対し、入力された安全性レベル情報ＳＬＩの表す安全性を達成し、かつ、復号エラーが発生しないＮＴＲＵ暗号のパラメータＰＳを生成することができる。

【０１７９】

＜実施の形態１における効果＞

従来の技術では、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータを生成するための条件が知られておらず、そのようなＮＴＲＵ暗号のパラメータを生成できなかった。そのため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができなかった。

【０１８０】

しかしながら、このパラメータ生成装置は、上述したように、理論的に復号エラーが発生しないようにパラメータｑを決定し、また入力された安全性レベルを達成するようにパラメータＮを決定するようにしたので、安全かつ理論的に復号エラーが発生しないＮＴＲＵ暗号のパラメータを生成できるようになった。

【０１８１】

（実施の形態２）

本発明に係る実施の形態２としてのパラメータ変換装置２について、実施の形態１との差異点を中心に説明する。

【０１８２】

＜パラメータ変換装置２の概要＞

最初に、図６を用いて本実施の形態の概要を説明する。

【０１８３】

このパラメータ変換装置２は、実施の形態１におけるパラメータ生成装置１を変形した構成したパラメータ変換装置であり、ＮＴＲＵ暗号のパラメータ組ＩＰ

Ｓとを入力としたとき、パラメータ組ＩＰＳを、総当りの探索による解読とＬＬＬアルゴリズムによる解読に対し、入力された安全性レベル情報ＳＬＩを達成し、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータ組ＰＳへ変換して出力する点が、パラメータ生成装置１と異なる。

【０１８４】

なお、実施の形態１におけるパラメータ生成装置１と同様にして、あるパラメータのＮＴＲＵ暗号の格子強度係数ＧＬ、その格子強度係数ＧＬを持つＮＴＲＵ暗号の解読時間評価式ＥＦ、及び復号エラーが発生しないパラメータの条件式ＥＤが予め与えられている。

【０１８５】

＜パラメータ変換装置２の構成＞

パラメータ変換装置２は、図６に示すように、入力部１０１ｂと、第２のパラメータ生成部１０３ｂと、第３のパラメータ生成部１０４ｂと、安全性判定部１０５と、安全性増加部１０６と、出力部１０７と、第１のパラメータ変更部１０８と、第２のパラメータ変更部１０９と、式格納部１１０から構成される。

【０１８６】

このパラメータ変換装置２は、入力部１０１ｂが異なることと、第１のパラメータ生成部が存在しないことと、第２のパラメータ生成部１０３ｂの入出力が異なることと、及び第３のパラメータ生成部１０４ｂの入出力が異なることとが、実施の形態１におけるパラメータ生成装置１と異なる。

【０１８７】

ここでは、パラメータ生成装置１との差異点を中心に説明を行う。

【０１８８】

（１）入力部１０１ｂ

入力部１０１ｂは、外部から安全性レベル情報ＳＬＩとＮＴＲＵ暗号のパラメータ組ＩＰＳを受け取り、安全性レベル情報ＳＬＩを第２のパラメータ生成部１０３ｂと安全性増加部１０６と第２のパラメータ変更部１０９に出力し、そして、パラメータ組ＩＰＳをパラメータ組ＰＳとして第３のパラメータ生成部１０４ｂへ出力する。

【０１８９】

（２）第２のパラメータ生成部１０３ｂ

第２のパラメータ生成部１０３ｂは、第１のパラメータ変更部１０８からパラメータ組ＰＳを受け取り、入力部１０１ｂから安全性レベル情報ＳＬＩを受け取る。そして、第２のパラメータ生成部１０３と同様にして、パラメータ候補集合ＤＳを生成する。そして、第２のパラメータ生成部１０３と同様にして、ＤＳの要素数がパラメータｄｆ、ｄｇ、ｄを選ぶのに不十分かどうか（例えば、要素数が３以上かどうか）を判別し、不十分だったら、パラメータ組ＰＳを第１パラメータ変更部１０８へ出力する。そうでなければ、パラメータｄｆ、ｄｇ、ｄを、パラメータ候補集合ＤＳから選び、選んだパラメータｄｆ、ｄｇ、ｄに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成してパラメータ組ＰＳを第３パラメータ生成部１０４ｂへ出力する。

【０１９０】

（３）第３のパラメータ生成部１０４ｂ

第３のパラメータ生成部１０４ｂは、入力部１０１ｂもしくは第２のパラメータ生成部１０３ｂからパラメータ組ＰＳを受け取り、式格納部１１０から復号エラーが発生しないパラメータの条件式ＥＤを読み取る。そして、第３のパラメータ生成部１０４と同様にして、パラメータ組ＰＳの中のパラメータｄｆ、ｄｇ、ｄに対し、条件式ＥＤを満たし、かつ、パラメータｑが２の冪となるような最小のｑをパラメータｑとして選ぶ。そして、選んだパラメータｑに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成し、パラメータ組ＰＳを安全性判定部１０５へ出力する。

【０１９１】

＜パラメータ変換装置２の動作＞

以上に述べたパラメータ変換装置２の動作について、図７、図８に示すフローチャートを用いて説明する。

【０１９２】

パラメータ変換装置２は、実施の形態１のパラメータ生成装置１と同様にして、あるパラメータのＮＴＲＵ暗号の格子強度係数ＧＬ、その格子強度係数ＧＬを

持つＮＴＲＵ暗号の解読時間評価式ＥＦ、及び復号エラーが発生しないパラメータの条件式ＥＤが予め与えられており、外部より安全性レベル情報ＳＬＩ及びＮＴＲＵ暗号のパラメータ組ＩＰＳが入力されると、以下の処理を行う。

【０１９３】

最初に、入力部１０１ｂは、外部から安全性レベル情報ＳＬＩとＮＴＲＵ暗号のパラメータ組ＩＰＳを受け取り、安全性レベル情報ＳＬＩを第２のパラメータ生成部１０３ｂと安全性増加部１０６と第２のパラメータ変更部１０９に出力し、パラメータ組ＩＰＳをパラメータ組ＰＳとして第３のパラメータ生成部１０４ｂへ出力し、処理をステップＳ２１０へ移す（ステップＳ２０１）。

【０１９４】

次に、第２のパラメータ生成部１０３ｂは、第１のパラメータ変更部１０８からパラメータ組ＰＳを受け取り、入力部１０１から安全性レベル情報ＳＬＩを受け取る（ステップＳ２０４）。

【０１９５】

そして、第２のパラメータ生成部１０３ｂは、パラメータ候補集合ＤＳを生成する（ステップＳ２０５）。

【０１９６】

そして、第２のパラメータ生成部１０３ｂは、ＤＳの要素数がパラメータｄｆ、ｄｇ、ｄを選ぶのに不十分かどうかを判別し、不十分だったら、処理をステップＳ２０７へ移す。そうでなければステップＳ２０９へ処理を移す（ステップＳ２０６）。

【０１９７】

そして、第２のパラメータ生成部１０３ｂは、パラメータ組ＰＳを第１パラメータ変更部１０８へ出力する。（ステップＳ２０７）。

【０１９８】

次に、第１のパラメータ変更部１０８は、第２のパラメータ生成部１０３ｂもしくは第２のパラメータ変更部１０９からパラメータ組ＰＳを受け取り、パラメータ組ＰＳの中のパラメータＮを増加させ、増加させたパラメータＮに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して第２のパラ

メータ生成部１０３ｂへ出力する。そして、処理をステップＳ２０４へ移す（ステップＳ２０８）。

【０１９９】

そして、第２のパラメータ生成部１０３ｂは、パラメータ候補集合ＤＳの要素からパラメータｄｆ、ｄｇ、ｄを選び、選んだパラメータｄｆ、ｄｇ、ｄに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して第３パラメータ生成部１０４ｂへ出力する（ステップＳ２０９）。

【０２００】

次に、第３のパラメータ生成部１０４ｂは、入力部１０１ｂからパラメータ組ＰＳを受け取り、式格納部１１０から復号エラーが発生しないパラメータの条件式ＥＤを読み取る（ステップＳ２１０）。

【０２０１】

そして、第３のパラメータ生成部１０４ｂは、パラメータ組ＰＳの中のパラメータｄｆ、ｄｇ、ｄに対し、条件式ＥＤを満たし、かつ、パラメータｑが２の冪となるような最小のｑをパラメータｑとして選び、選んだパラメータｑに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成して安全性判定部１０５へ出力する（ステップＳ２１１）。

【０２０２】

次に、安全性判定部１０５は、第３のパラメータ生成部１０４ｂもしくは第２のパラメータ変更部１０９からパラメータ組ＰＳを受け取り、パラメータ組ＰＳの中のパラメータＮ、ｐ、ｑ、ｄｆ、ｄｇをもつＮＴＲＵ暗号の格子強度係数ＳＬを導出する（ステップＳ２１２）。

【０２０３】

そして、安全性判定部１０５は、式格納部１１０から格子強度係数ＧＬを読み取り、ＧＬ≦ＳＬならば、ステップＳ２１４へ処理を移す。そうでなければ、ステップＳ２２３へ処理を移す（ステップＳ２１３）。

【０２０４】

そして、安全性判定部１０５は、パラメータ組ＰＳを安全性増加部１０６へ出力する（ステップＳ２１４）。

【０２０５】

次に、安全性増加部１０６は、安全性判定部１０５からパラメータ組ＰＳを受け取り、入力部１０１ｂから安全性レベル情報ＳＬＩを受け取り、式格納部１１０より解読時間評価式ＥＦを読み取る（ステップＳ２１５）。

【０２０６】

そして、安全性増加部１０６は、パラメータ組ＰＳの中のパラメータＮと解読時間評価式ＥＦからＮＴＲＵ暗号の解読時間Ｔを導出する（ステップＳ２１６）。

【０２０７】

そして、安全性増加部１０６は、導出した解読時間Ｔが、Ｔ＜ＳＬＩならば、ステップＳ２１８へ処理を移す。そうでなければ、ステップＳ２１９へ処理を移す（ステップＳ２１７）。

【０２０８】

そして、安全性増加部１０６は、解読時間ＴがＴ≧ＳＬＩとなるようにパラメータＮを増加させ、増加させたパラメータＮに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成する（ステップＳ２１８）。

【０２０９】

そして、安全性増加部１０６は、パラメータＮが素数であれば、ステップＳ２２１へ処理を移す。そうでなければステップＳ２２０へ処理を移す（ステップＳ２１９）。

【０２１０】

そして、安全性増加部１０６は、パラメータＮを増加させ、増加させたパラメータＮが素数となるようにし、増加させたパラメータＮに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成する（ステップＳ２２０）。

【０２１１】

そして、安全性増加部１０６は、パラメータ組ＰＳを出力部１０７へ出力する（ステップＳ２２１）。

【０２１２】

次に、出力部１０７は、安全性増加部１０６からパラメータ組ＰＳを受け取り

、パラメータ組ＰＳを外部へ出力して処理を終了する（ステップＳ２２２）。

【０２１３】

次に、第２のパラメータ変更部１０９は、入力部１０１ｂから安全性レベル情報ＳＬＩを受け取り、安全性判定部１０５からパラメータ組ＰＳを受け取り、パラメータ候補集合ＤＳを生成する（ステップＳ２２３）。

【０２１４】

そして、第２のパラメータ変更部１０９は、パラメータ組ＰＳの中のパラメータｄｇとパラメータ候補集合ＤＳの要素の最大値Ｍを比較し、ｄｇ＜Ｍであれば、処理をステップＳ２２５へ移す。そうでなければ、ステップＳ２２６へ処理を移す（ステップＳ２２４）。

【０２１５】

そして、第２のパラメータ変更部１０９は、パラメータｄｇを、パラメータ候補集合ＤＳの要素のうち、より大きい値に変更し、変更したパラメータｄｇに対し、新たにパラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）を生成し、パラメータ組ＰＳを安全性判定部１０５へ出力して、処理をステップＳ２１２へ移す（ステップＳ２２５）。

【０２１６】

そして、第２のパラメータ変更部１０９は、パラメータ組ＰＳを第１のパラメータ変更部１０８へ出力して、処理をステップＳ２０８へ移す（ステップＳ２２６）。

【０２１７】

＜パラメータ変換装置２の動作検証＞

以下に、実施の形態２におけるパラメータ変換装置２の全体の動作について説明する。

【０２１８】

まず、入力部１０１ｂが、ステップＳ２０１において、入力されたＮＴＲＵ暗号のパラメータ組ＩＰＳをパラメータ組ＰＳとして第３のパラメータ生成部１０４ｂに出力している。

【０２１９】

そして、第２のパラメータ生成部１０３ｂは、実施の形態１と同様にして、ＮＴＲＵ暗号を総当りで探索する解読に対し、安全性レベル情報ＳＬＩの表す安全性レベルを達成するパラメータ候補集合ＤＳを生成する（ステップＳ２０５）。

【０２２０】

そして、第３のパラメータ生成部１０４が、ステップＳ２１１において、復号エラーが発生しないパラメータの条件式ＥＤを満たすように、パラメータｑを選ぶことにより、パラメータ組ＰＳ＝（Ｎ，ｐ，ｑ，ｄｆ，ｄｇ，ｄ）の値が決まる。

【０２２１】

ここで、実施の形態１と同様に、パラメータｑの値を、条件式ＥＤを満たすように選ぶと、ＬＬＬアルゴリズムによる解読に対する安全性レベル（解読時間）が下がる可能性があるので、予め格納されている格子強度係数ＧＬに基づき、安全性判定部１０５が、ステップＳ２１３において、生成されたパラメータ組ＰＳをもつＮＴＲＵ暗号の解読時間が、その格子強度係数ＧＬに基づく解読時間評価式ＥＦで評価可能かどうかを判断し、そして、評価可能であれば、安全性増加部１０６が、ステップＳ２１８において、安全性レベル情報ＳＬＩの表す安全性レベルを達成するようにパラメータＮを増加させている。

【０２２２】

なお、そうでない場合には、第２のパラメータ変更部１０９が、ステップＳ２２５において、パラメータｄｇをより大きい値にすることにより、そのパラメータをもつＮＴＲＵ暗号の格子強度係数の値を大きくして、解読時間評価式ＥＦで評価できるようにするか、それで対応できない場合は、第１のパラメータ変更部１０８が、ステップＳ２０８で、パラメータＮを増加させ、そしてステップＳ２０９以降で、もう一度パラメータｄｆ、ｄｇ、ｄ、ｑの生成を行うようにしている。

【０２２３】

今、パラメータＮを大きくとれば、一般にパラメータ候補集合ＤＳは大きい要素をもつようになる。よって、ステップＳ２０９で、パラメータｄｆ、ｄｇ、ｄをもう一度選び直すときには、ｄｆ、ｄの値を変えずに、ｄｇのみ値を大きくと

ることができる。そして、ｄｇの値は、復号エラー発生の条件式には関与しないので、復号エラーが発生しないことを保証したまま、安全強度指標ＧＬの値を大きくして、解読時間評価式ＥＦで評価できるようにすることが可能となる。

【０２２４】

以上により、高々有限回の繰り返し回数で、入力されたＮＴＲＵ暗号のパラメータＩＰＳを、総当りの探索による解読とＬＬＬアルゴリズムによる解読に対し、入力された安全性レベル情報ＳＬＩの表す安全性レベルを達成し、かつ、復号エラーが発生しないＮＴＲＵ暗号のパラメータＰＳに変換することができる。

【０２２５】

＜実施の形態２における効果＞

従来の技術では、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータを生成するための条件が知られておらず、そのようなＮＴＲＵ暗号のパラメータを生成できなかった。そのため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができなかった。

【０２２６】

しかしながら、このパラメータ変換装置は、上述したように、入力されたＮＴＲＵ暗号のパラメータに対し、理論的に復号エラーが発生しないようにパラメータｑを決定し、また入力された安全性レベルを達成するようにパラメータＮを決定するようにしたので、安全でかつ理論的に復号エラーが発生しないＮＴＲＵ暗号のパラメータに変換できるようになった。

【０２２７】

（実施の形態３）

本発明に係る実施の形態３としての暗号システム３について説明する。

【０２２８】

＜暗号システム３の構成＞

この暗号システム３は、図１１に示すように、暗号装置３１、復号装置３２、及び通信路３３から構成され、実施の形態１におけるパラメータ生成装置１あるいは実施の形態２におけるパラメータ変換装置２によって生成された、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号の

パラメータを利用して、暗号化通信を行うシステムである。

【０２２９】

＜暗号装置３１の構成＞

暗号装置３１は、図１２に示すように、パラメータ記憶部３１１、公開鍵記憶部３１２、暗号化部３１３から構成される。

【０２３０】

（１）パラメータ記憶部３１１

パラメータ記憶部３１１は、実施の形態１におけるパラメータ生成装置１あるいは実施の形態２におけるパラメータ変換装置２によって生成されたＮＴＲＵ暗号のパラメータである、パラメータＮ、パラメータｐ、パラメータｑ、パラメータｄｆ、パラメータｄｇ、パラメータｄを、予め記憶している。

【０２３１】

（２）公開鍵記憶部３１２

公開鍵記憶部３１１は、予め復号装置３２の公開鍵多項式ｈを取得し、記憶している。

【０２３２】

この公開鍵多項式ｈは、パラメータＮに対し、Ｎ－１次元以下の多項式で表される多項式である。

【０２３３】

（３）暗号化部３１３

暗号化部３１３は、パラメータ記憶部３１１からパラメータＮ、パラメータｐ、パラメータｑ、パラメータｄを受け取り、公開鍵記憶部３１２から、公開鍵多項式ｈを受け取り、外部から、パラメータＮに対し、Ｎ－１次元以下の多項式で表される平文多項式ｍを受け取る。

【０２３４】

そして、パラメータＮ、パラメータｄを用いて、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつ他の係数は０となるように、Ｎ－１次元の乱数多項式ｒをランダムに選ぶ。

【０２３５】

そして、平文多項式ｍに対し、乱数多項式ｒ、公開鍵多項式ｈ、パラメータＮ、パラメータｐ、パラメータｑを用いて、ＮＴＲＵ暗号の暗号化処理を行い、暗号文多項式ｃを計算する。

【０２３６】

この暗号文多項式ｃの演算方法の詳細は、非特許文献２に記載されているため、ここでは説明を省略する。そして、生成した暗号文多項式ｃを通信路３３を介して復号装置３２へ送信する。

【０２３７】

＜復号装置３２の構成＞

復号装置３２は、図１３に示すように、パラメータ記憶部３２１、鍵生成部３２２、秘密鍵記憶部３２３、復号化部３２４から構成される。

【０２３８】

（１）パラメータ記憶部３２１

パラメータ記憶部３２１は、暗号装置３１のパラメータ記憶部３１１が記憶するＮＴＲＵ暗号のパラメータと同じＮＴＲＵ暗号のパラメータを記憶している。

【０２３９】

すなわち、パラメータ記憶部３１１が記憶するものと同じパラメータＮ、パラメータｐ、パラメータｑ、パラメータｄｆ、パラメータｄｇ、パラメータｄを、予め記憶している。

【０２４０】

（２）鍵生成部３２２

鍵生成部３２２は、パラメータ記憶部３２１からパラメータＮ、パラメータｐ、パラメータｑ、パラメータｄｆ、パラメータｄｇを受け取り、パラメータＮ、パラメータｐ、パラメータｑ、パラメータｄｆ、パラメータｄｇを用いて、Ｎ－１次元以下の多項式で表される秘密鍵多項式ｆ、及び公開鍵多項式ｈを生成する。なお、この秘密鍵多項式ｆ及び公開鍵多項式ｈの生成方法は、非特許文献２に記載されているため、ここでは説明を省略する。

【０２４１】

そして、公開鍵多項式ｈを公開して暗号装置３１が取得できるようにし、秘密

鍵多項式ｆを秘密鍵記憶部３２３に記憶する。

【０２４２】

（３）秘密鍵記憶部３２３

秘密鍵記憶部３２３は、予め復号装置３２の秘密鍵多項式ｆを記憶している。

【０２４３】

この秘密鍵多項式ｆは、パラメータＮに対し、Ｎ－１次元以下の多項式で表される多項式である。

【０２４４】

（４）復号化部３２４

復号化部３２４は、パラメータ記憶部３２１から、パラメータＮ、パラメータｐ、パラメータｑを受け取り、秘密鍵記憶部３２３から、秘密鍵多項式ｆを受け取り、通信路３３を介して暗号装置３１から暗号文多項式ｃを受け取る。

【０２４５】

そして、暗号文多項式ｃに対し、秘密鍵多項式ｆ、パラメータＮ、パラメータｐ、パラメータｑを用いて、ＮＴＲＵ暗号の復号化処理を行い、復号文多項式ｍ’を計算する。このＮＴＲＵ暗号の復号化処理の詳細は、非特許文献２に記載されているため、ここでは説明を省略する。

【０２４６】

そして、生成した復号文多項式ｍ’を外部へ出力する。

【０２４７】

＜暗号システム３の動作＞

以上に述べた暗号システム３の動作について説明する。

【０２４８】

暗号システム３は、実施の形態１におけるパラメータ生成装置１あるいは実施の形態２におけるパラメータ変換装置２によって生成された、ＮＴＲＵ暗号のパラメータに対し、少なくとも、パラメータＮ、パラメータｐ、パラメータｑ、パラメータｄを暗号装置３１のパラメータ記憶部３１１に記憶しており、少なくともパラメータＮ、パラメータｐ、パラメータｑ、パラメータｄｆ、パラメータｄｇを復号装置３２のパラメータ記憶部３２１に記憶している（ステップＳ３０１

）。

【０２４９】

そして、復号装置３２の鍵生成部３２２は、パラメータ記憶部３２１からパラメータＮ、パラメータｐ、パラメータｑ、パラメータｄｆ、パラメータｄｇを受け取り、秘密鍵多項式ｆ、及び公開鍵多項式ｈを生成して、公開鍵多項式ｈを公開して暗号装置３１が取得できるようにし、秘密鍵多項式ｆを秘密鍵記憶部３２３に記憶する（ステップＳ３０２）。

【０２５０】

そして、暗号装置３１の公開鍵記憶部３１２は、復号装置３２の公開鍵多項式ｈを取得し記憶する（ステップＳ３０３）。

【０２５１】

そして、暗号装置３１の暗号化部３１３は、パラメータ記憶部３１１からパラメータＮ、パラメータｐ、パラメータｑ、パラメータｄを受け取り、公開鍵記憶部３１２から、公開鍵多項式ｈを受け取り、外部から、パラメータＮに対し、Ｎ－１次元以下の多項式で表される平文多項式ｍを受け取る（ステップＳ３０４）。

【０２５２】

そして、暗号装置３１の暗号化部３１３は、パラメータＮ、パラメータｄを用いて、ｄ個の係数が１であり、かつｄ個の係数が－１であり、かつ他の係数は０となるように、Ｎ－１次元の乱数多項式ｒをランダムに選び、平文多項式ｍに対し、乱数多項式ｒ、公開鍵多項式ｈ、パラメータＮ、パラメータｐ、パラメータｑを用いて、ＮＴＲＵ暗号の暗号化処理を行い、暗号文多項式ｃを計算する（ステップＳ３０５）。

【０２５３】

そして、暗号装置３１の暗号化部３１３は、暗号文多項式ｃを通信路３３を介して復号装置３２へ送信する（ステップＳ３０６）。

【０２５４】

そして、復号装置３２の復号化部３２４は、パラメータ記憶部３２１から、パラメータＮ、パラメータｐ、パラメータｑを受け取り、秘密鍵記憶部３２３から

、秘密鍵多項式ｆを受け取り、通信路３３を介して暗号装置３１から暗号文多項式ｃを受け取る（ステップＳ３０７）。

【０２５５】

そして、復号装置３２の復号化部３２４は、暗号文多項式ｃに対し、秘密鍵多項式ｆ、パラメータＮ、パラメータｐ、パラメータｑを用いて、ＮＴＲＵ暗号の復号化処理を行い、復号文多項式m’を計算する（ステップＳ３０８）。

【０２５６】

そして、復号装置３２の復号化部３２４は、復号文多項式m’を外部へ出力すして処理を終了する（ステップＳ３０９）。

【０２５７】

＜暗号システム３の動作検証＞

まず、復号装置３２は、ステップＳ３０２において、実施の形態１におけるパラメータ生成装置１あるいは実施の形態２におけるパラメータ変換装置によって生成されたＮＴＲＵ暗号のパラメータを用いて、秘密鍵多項式ｆ、公開鍵多項式ｈを生成している。

【０２５８】

そして、暗号装置３１が、ステップＳ３０５において、実施の形態１におけるパラメータ生成装置１あるいは実施の形態２におけるパラメータ変換装置によって生成されたＮＴＲＵ暗号のパラメータを用いて、平文多項式ｍを暗号化している。

【０２５９】

以上により、実施の形態１におけるパラメータ生成装置１あるいは実施の形態２におけるパラメータ変換装置２によって生成されたパラメータを用いて、秘密鍵多項式ｆ、公開鍵多項式ｈを生成して暗号化を行っているため、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないことがいえる。

【０２６０】

＜実施の形態３における効果＞

従来の技術では、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータを生成するための条件が知られておらず

、そのようなＮＴＲＵ暗号のパラメータを生成できなかった。そのため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができなかった。

【０２６１】

しかしながら、この暗号システムは、上述したように、実施の形態１におけるパラメータ生成装置１あるいは実施の形態２におけるパラメータ変換装置２によって生成されたパラメータを用いて、秘密鍵多項式ｆ、公開鍵多項式ｈを生成して暗号化をおこなっているため、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるようになった。

【０２６２】

＜変形例＞

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

【０２６３】

（１）式格納部１１０に格納される格子強度係数ＧＬ及び解読時間評価式ＥＦは、図１０に示す通り複数の組が格納され、安全性判定部１０５がＧＬ≦ＳＬを満たす格子強度係数ＧＬと解読時間評価式ＥＦの組を読み取ってもよい。

【０２６４】

また、式格納部１１０に格納される格子強度係数ＧＬ及び解読時間評価式ＥＦは、後で変更できるようにしてもよい。

【０２６５】

（２）第１のパラメータ生成部１０２におけるパラメータＮの選択方法は、この方法に限定されず、Ｎが十分大きくとれる方法であれば任意の方法でよい。例えば、Ｆ（ｘ）＝１０・ｌｏｇ（ｘ）等の単調増加関数Ｆに対し、Ｎ＝Ｆ（ＳＬＩ）によって選択してもよい。また、例えば、パラメータＮは固定値であってもよい。

【０２６６】

（３）第２のパラメータ生成部１０３におけるパラメータｄｆ、ｄｇ、ｄの選択方法は、この方法に限定されず、総当りで探索する解読に対し、秘密鍵の安全

性レベルと平文の安全性レベルが安全性レベル情報ＳＬＩが表す安全性レベルを達成し、かつｄｇ＞ｄとなるように選択すれば、どのような方法でもよい。

【０２６７】

（４）また、パラメータ組ＰＳの中のパラメータｑ、ｄｆ、ｄｇ、ｄは、第２のパラメータ生成部１０３が上述の方法でパラメータｄｆ、ｄｇ、ｄを選択し、第３のパラメータ生成部１０４が条件式ＥＤにパラメータｄｆ、ｄｇ、ｄの値を適用してパラメータｑの値を決定することにより生成する以外にも、パラメータｑが外部から予め与えられており、条件式ＥＤとパラメータｑの値から導出される関係式に基づいて、ｄｇ＞ｄとなるようにパラメータｄｆ、ｄｇ、ｄを選択することにより生成してもよい。

【０２６８】

具体的には、例えばパラメータｑとしてｑ＝２５６が外部から予め与えられている場合、条件式ＥＤとパラメータｑの値から、

６ｄ＋２ｄｆ－１＜１２８

という関係式を満たし、かつｄｇ＞ｄとなるようにパラメータｄｆ、ｄｇ、ｄを選び、パラメータ組ＰＳの中のパラメータｑ、ｄｆ、ｄｇ、ｄを生成してもよい。

【０２６９】

なお、この場合、パラメータｄｆ、ｄｇ、ｄは、総当りで探索する解読に対し、秘密鍵や平文の解読時間が安全性レベル情報ＳＬＩが表す安全性レベルを達成していない可能性がある。そのため、安全性増加部１０６が、上述のように、ＬＬＬアルゴリズムによる解読時間Ｔが安全性レベル情報ＳＬＩを達成するようにパラメータＮを増加させた後、第２のパラメータ生成部１０３の構成において説明した秘密鍵や平文を総当りで探索する暗号解読の解読時間が、安全性レベル情報ＳＬＩが表す安全性レベルを達成するようにパラメータＮを増加してもよい。

【０２７０】

また、秘密鍵や平文を総当りで探索する暗号解読の解読時間が、安全性レベル情報ＳＬＩが表す安全性レベルを達成するようにパラメータＮを増加させた後、ＬＬＬアルゴリズムによる解読時間Ｔが安全性レベル情報ＳＬＩを達成するよう

にパラメータＮを増加させてもよい。

【０２７１】

（５）第３のパラメータ生成部１０４におけるパラメータｑの選択方法は、この方法に限定されず、条件式ＥＤを満たし、かつパラメータｐと互いに素になるように選択すれば、どのような方法でもよい。

【０２７２】

（６）第１のパラメータ生成部１０２が生成するパラメータｐ、及びパラメータ変換装置２が扱うパラメータ組ＩＰＳ、ＰＳの中のパラメータｐは、ｐ＝３に限定されず、他のものでもよい。

【０２７３】

例えば、ある非負整数ｋに対してｐ＝ｋとした場合、式格納部１１０に格納される条件式ＥＤを

ＥＤ：２・ｋ・ｄ＋２ｄｆ－１＜ｑ／２

とすれば、同様の効果が得られる。

【０２７４】

（７）上記変形例（６）に関し、さらに、ある多項式ｂに対してｐ＝ｂとしてもよい。例えば、ｐ＝（Ｘ＋２）とした場合、

この場合、式格納部１１０に格納される条件式ＥＤを

ＥＤ：６ｄ＋２ｄｆ－１＜ｑ／２

とすれば、同様の効果が得られる。

【０２７５】

何故ならば、上述した通り、多項式ｐ×ｒ×ｇ＋ｆ×ｍの全ての係数が、－ｑ／２からｑ／２の範囲に収まっていれば、復号エラーは発生しないのであった。

【０２７６】

このとき、多項式ｒ×ｇを考えると、その係数の最大値は、高々２ｄであった（最小値も、せいぜい－２ｄ。）。

【０２７７】

今、ｐ＝（Ｘ＋２）なので、多項式ａのｋ次の係数をａ（ｋ）で表すと、

ｐ（０）＝２、ｐ（１）＝１、ｐ（ｉ）＝０　（ｉ＞１）

であるので、

（ｐ×（ｒ×ｇ））（ｋ）
＝ｐ（０）・（ｒ×ｇ）（ｋ）＋ｐ（１）・（ｒ×ｇ）（ｋ－１）＋
．．．＋ｐ（Ｎ－１）・（ｒ×ｇ）（ｋ－（Ｎ－１）（ｍｏｄ　Ｎ））
＝（ｒ×ｇ）（ｋ）＋２・（ｒ×ｇ）（ｋ－１）

である。

【０２７８】

よって、多項式ｐ×ｒ×ｇを考えると、その係数の最大値は、３・２ｄである。一方、多項式ｆ×ｍの係数の値は、その値が高々２ｄｆ－１であった（最小値も、せいぜい－２ｄｆ＋１。）。

【０２７９】

従って、実施の形態で説明したのと同様にして、多項式ｐ×ｒ×ｇ＋ｆ×ｍの最も大きい係数の値は、高々３・２ｄ＋２ｄｆ－１であることが導くことができ、ここから、復号エラーが理論的に発しない条件式ＥＤとして、

ＥＤ：６ｄ＋２ｄｆ－１＜ｑ／２

を導くことができる。

【０２８０】

なお、多項式ｂはｂ＝（Ｘ＋２）に限定されないことはもちろんである。その場合、上述の処理を行えば、条件式ＥＤを導くことができて、同様の効果が得られる。

【０２８１】

（８）なお、パラメータ変換装置２において、パラメータ組ＩＰＳを外部より入力する以外にも、入力部１０１ｂが、安全性レベル情報ＳＬＩが表す安全性レベルを達成する、パラメータ組ＩＰＳのリストを保持して、外部よりの入力安全性レベル情報ＳＬＩだけにしてもよい。すなわち、入力部１０１ｂが、図９に示すようなパラメータ組ＩＰＳのリストを保持しており、外部から安全性レベル情報ＳＬＩが入力されると、このＳＬＩに関連付けられたパラメータ組ＩＰＳをパラメータ組ＰＳとして第３のパラメータ生成部１０５へ出力してもよい。

【０２８２】

（９）なお、非特許文献４には、Ｚｅｒｏ－Ｒｕｎ　Ｌａｔｔｉｃｅを用いる解読により、ＬＬＬアルゴリズムの解読時間が減少する可能性があることが記載されているが、解読時間評価式ＥＦは、このＺｅｒｏ－Ｒｕｎ　Ｌａｔｔｉｃｅを用いた解読を考慮した、ＬＬＬアルゴリズムの解読時間としてもよい。

【０２８３】

（１０）なお、暗号システム３において、秘密鍵多項式ｆ及び公開鍵多項式ｈは、復号装置３２の鍵生成部３２２で生成される以外にも、これらが例えば鍵管理サーバ等の復号装置３２の外部で生成されて、秘密鍵多項式ｆが、外部から秘密鍵記憶部３２３へ入力され、公開鍵多項式ｈが、外部から公開鍵記憶部３１２へ入力されるようにしてもよい。

【０２８４】

（１１）なお、暗号システム３において、暗号システム３は、さらに実施の形態１におけるパラメータ生成装置１、あるいは実施の形態２におけるパラメータ変換装置２を備え、パラメータ生成装置１あるいはパラメータ変換装置２が出力したＮＴＲＵ暗号のパラメータが、パラメータ記憶部３１１、３２１に入力されるようにしてもよい。

【０２８５】

（１２）変形例（１１）に関し、暗号システム３において、暗号装置３１が、さらに、実施の形態１におけるパラメータ生成装置１あるいはパラメータ変換装置２の構成要素を含み、暗号装置３１がＮＴＲＵ暗号のパラメータを生成し、生成したＮＴＲＵ暗号のパラメータが、パラメータ記憶部３１１に入力され、通信路３３を介して復号装置３２へ送信され、復号装置３２で受信されたこのＮＴＲＵ暗号のパラメータがパラメータ記憶部３２１に入力されるようにしてもよい。

【０２８６】

（１３）パラメータ記憶部３１１に記憶されるＮＴＲＵ暗号パラメータは、パラメータＮ、ｐ、ｑ、ｄｆ、ｄｇ、ｄのうち、少なくとも、パラメータＮ、パラメータｐ、パラメータｑ、パラメータｄを含めば、どのようなものでもよい。また、パラメータ記憶部３２１に記憶されるＮＴＲＵ暗号パラメータは、少なくとも、パラメータＮ、パラメータｐ、パラメータｑ、パラメータｄｆ、パラメータ

ｄｇを含めば、どのようなものでもよい。

【０２８７】

（１４）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０２８８】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、半導体メモリ、ハードディスクドライブ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ等、に記録したものとしてもよい。

【０２８９】

（１５）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０２９０】

【発明の効果】

以上に説明したように、本発明は、従来技術における問題点を鑑みて行われたもので、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるように、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータを生成するパラメータ生成装置を構成することができるようになった。

【０２９１】

また、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができるように、入力されたＮＴＲＵ暗号のパラメータに対し、第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータに変換するパラメータ変換装置を構成できるようになった。

【０２９２】

さらに、これらのパラメータ装置もしくはパラメータ変換装置により生成されたパラメータを用いて、暗号装置と復号装置との間で安全かつ確実な暗号化通信ができる、暗号システム、暗号装置及び復号装置を構成できるようになった。

【０２９３】

以上により、従来技術では達成できなかったパラメータ生成装置、パラメータ変換装置、暗号システム、暗号装置、及び復号装置を提供することができ、その価値は大きい。

【図面の簡単な説明】

【図１】

本発明の実施の形態１におけるパラメータ生成装置１の構成を示す図

【図２】

パラメータＮにおける解読時間Ｔの実測データを示す図

【図３】

本発明の実施の形態１における式格納部１１０の構成を示す図

【図４】

本発明の実施の形態１におけるパラメータ生成装置１の処理の前半部を表す図

【図５】

本発明の実施の形態１におけるパラメータ生成装置１の処理の後半部を表す図

【図６】

本発明の実施の形態２におけるパラメータ変換装置２の構成を示す図

【図７】

本発明の実施の形態２におけるパラメータ変換装置２の処理の前半部を示す図

【図８】

本発明の実施の形態２におけるパラメータ変換装置２の処理の後半部を示す図

【図９】

安全性レベル情報とその安全性レベルを達成するＮＴＲＵ暗号のパラメータ組を示す図

【図１０】

本発明の変形例（１）における式格納部１１０の構成を示す図

【図１１】

本発明の実施の形態３における暗号システム３の構成を示す図

【図１２】

本発明の実施の形態３における暗号装置３１の構成を示す図

【図１３】

本発明の実施の形態３における復号装置３２の構成を示す図

【符号の説明】

１　パラメータ生成装置

２　パラメータ変換装置

３　暗号システム

３１　暗号装置

３２　復号装置

３３　通信路

１０１，１０１ｂ　入力部

１０２　第１のパラメータ生成部

１０３，１０３ｂ　第２のパラメータ生成部

１０４，１０４ｂ　第３のパラメータ生成部

１０５　安全性判定部

１０６　安全性増加部

１０７　出力部

１０８　第１のパラメータ変更部

１０９　第２のパラメータ変更部

１１０　式格納部

３１１，３２１　パラメータ記憶部

３１２　公開鍵記憶部

３１３　暗号化部

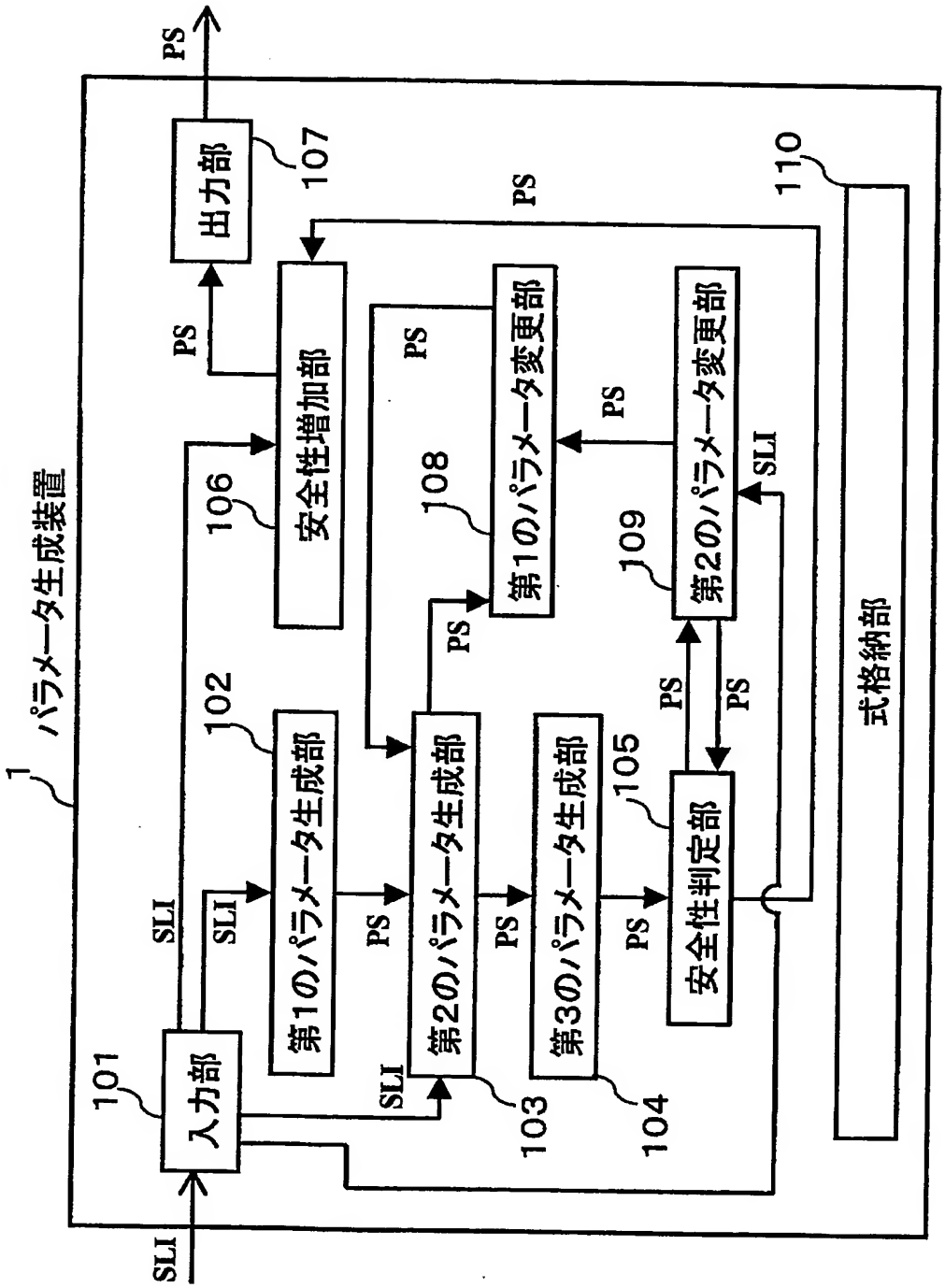
３２２　鍵生成部

３２３　秘密鍵記憶部

３２４　復号化部

【書類名】　図面

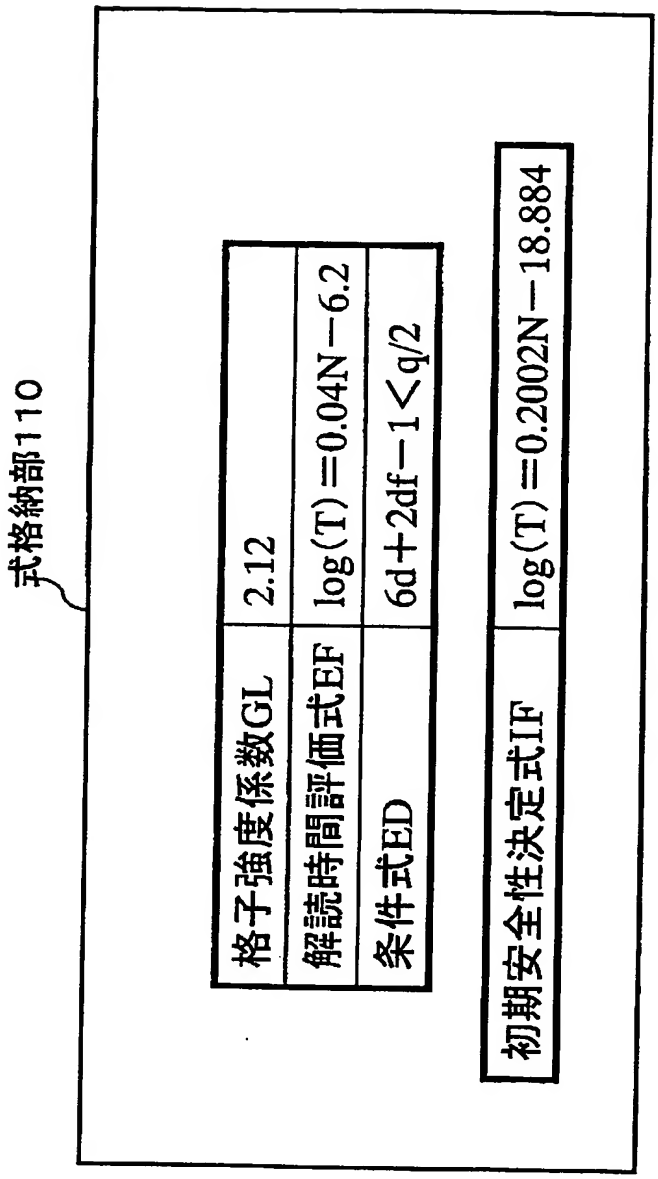
【図１】


1
パラメータ生成装置
101
入力部
102
第1のパラメータ生成部
103
第2のパラメータ生成部
104
第3のパラメータ生成部
105
安全性判定部
106
安全性増加部
107
出力部
108
第1のパラメータ変更部
109
第2のパラメータ変更部
110
式格納部
SLI
PS

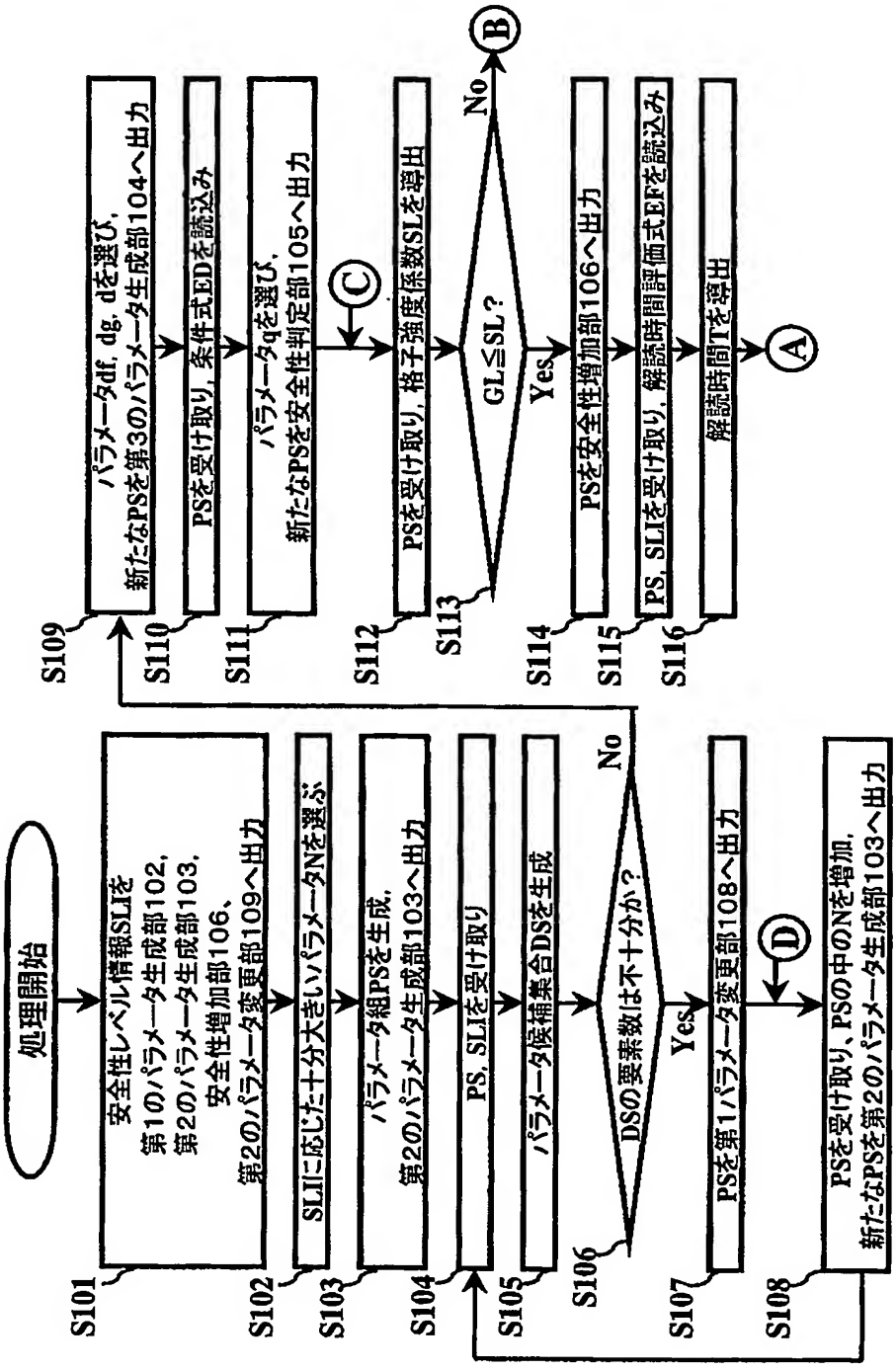
【図２】

パラメータN	解読時間T(秒)
70	16.587
72	18.68
74	26.497
76	25.869
78	31.182
80	37.76
82	56.442
84	56.359
86	68.174
88	86.6
90	111.78

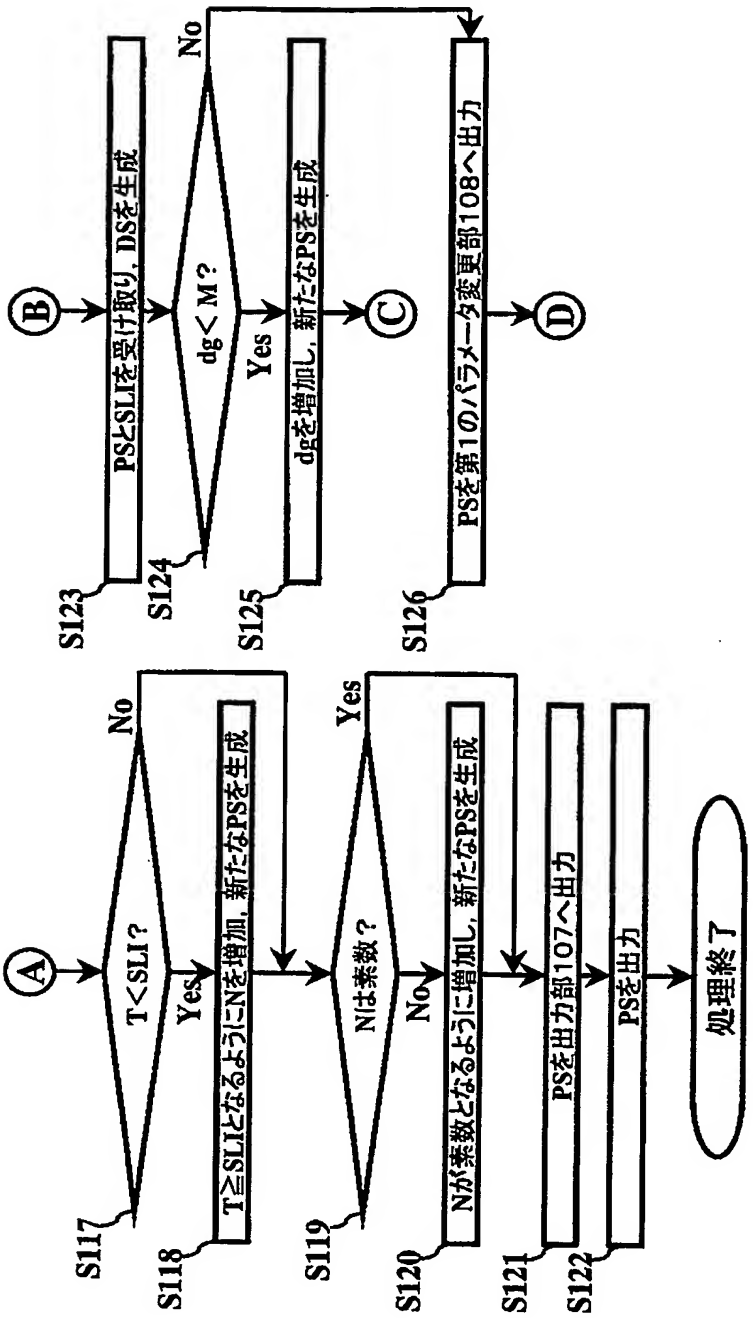
【図３】


式格納部110
格子強度係数GL
2.12
解読時間評価式EF
log(T)=0.04N−6.2
条件式ED
6d+2df−1<q/2
初期安全性決定式IF
log(T)=0.2002N−18.884

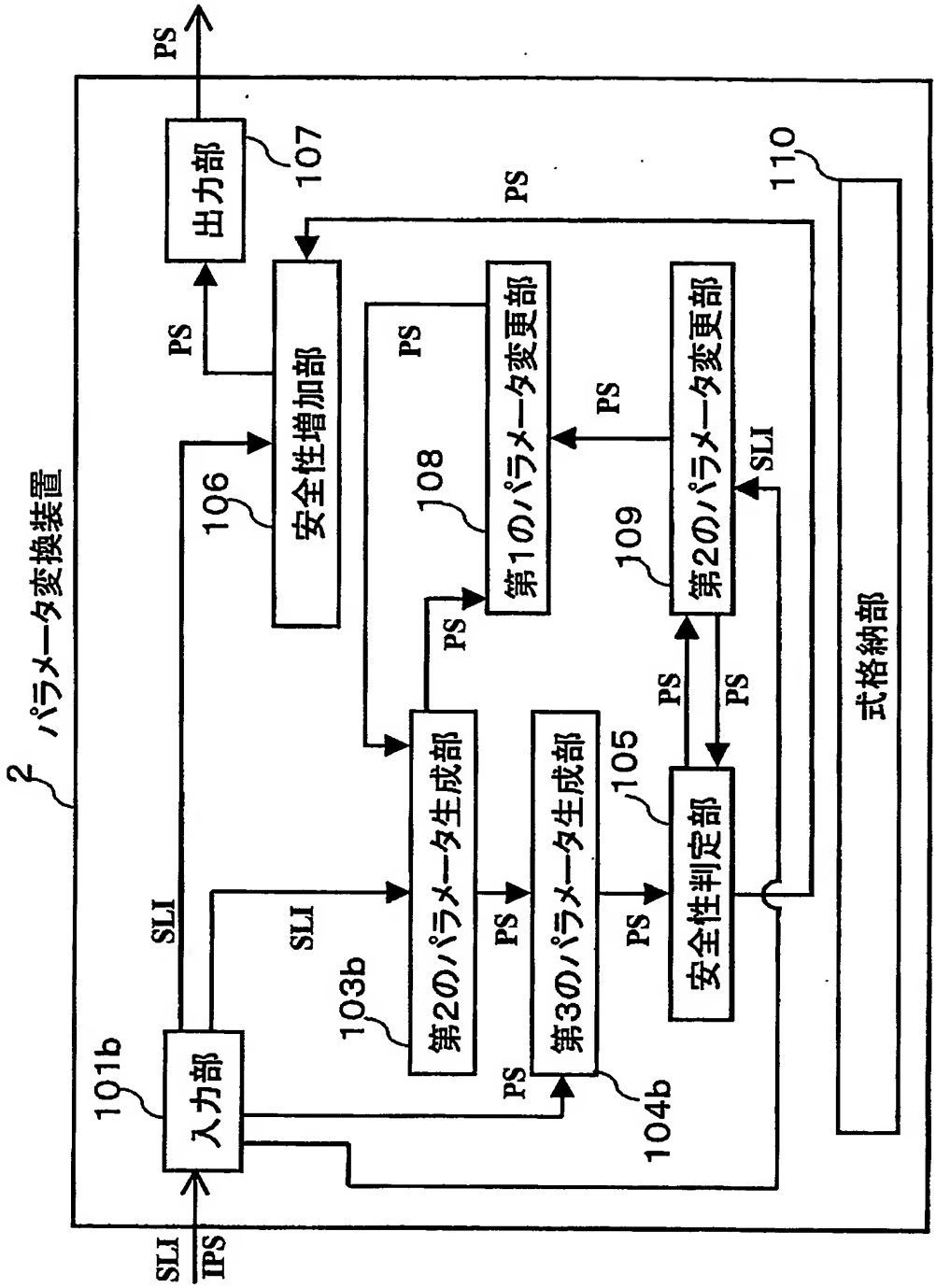
【図４】


処理開始
安全性レベル情報SLIを
第1のパラメータ生成部102,
第2のパラメータ生成部103,
安全性増加部106,
第2のパラメータ変更部109へ出力
S101
SLIに応じた十分大きいパラメータNを選ぶ
S102
パラメータ組PSを生成,
第2のパラメータ生成部103へ出力
S103
PS, SLIを受け取り
S104
パラメータ候補集合DSを生成
S105
DSの要素数は不十分か?
S106
No
Yes
PSを第1パラメータ変更部108へ出力
S107
D
PSを受け取り、PSの中のNを増加,
新たなPSを第2のパラメータ生成部103へ出力
S108
パラメータdf, dg, dを選び,
新たなPSを第3のパラメータ生成部104へ出力
S109
PSを受け取り, 条件式EDを読込み
S110
パラメータqを選び,
新たなPSを安全性判定部105へ出力
S111
C
PSを受け取り, 格子強度係数SLを導出
S112
GL≦SL?
S113
No
B
Yes
PSを安全性増加部106へ出力
S114
PS, SLIを受け取り, 解読時間評価式EFを読込み
S115
解読時間Tを導出
S116
A

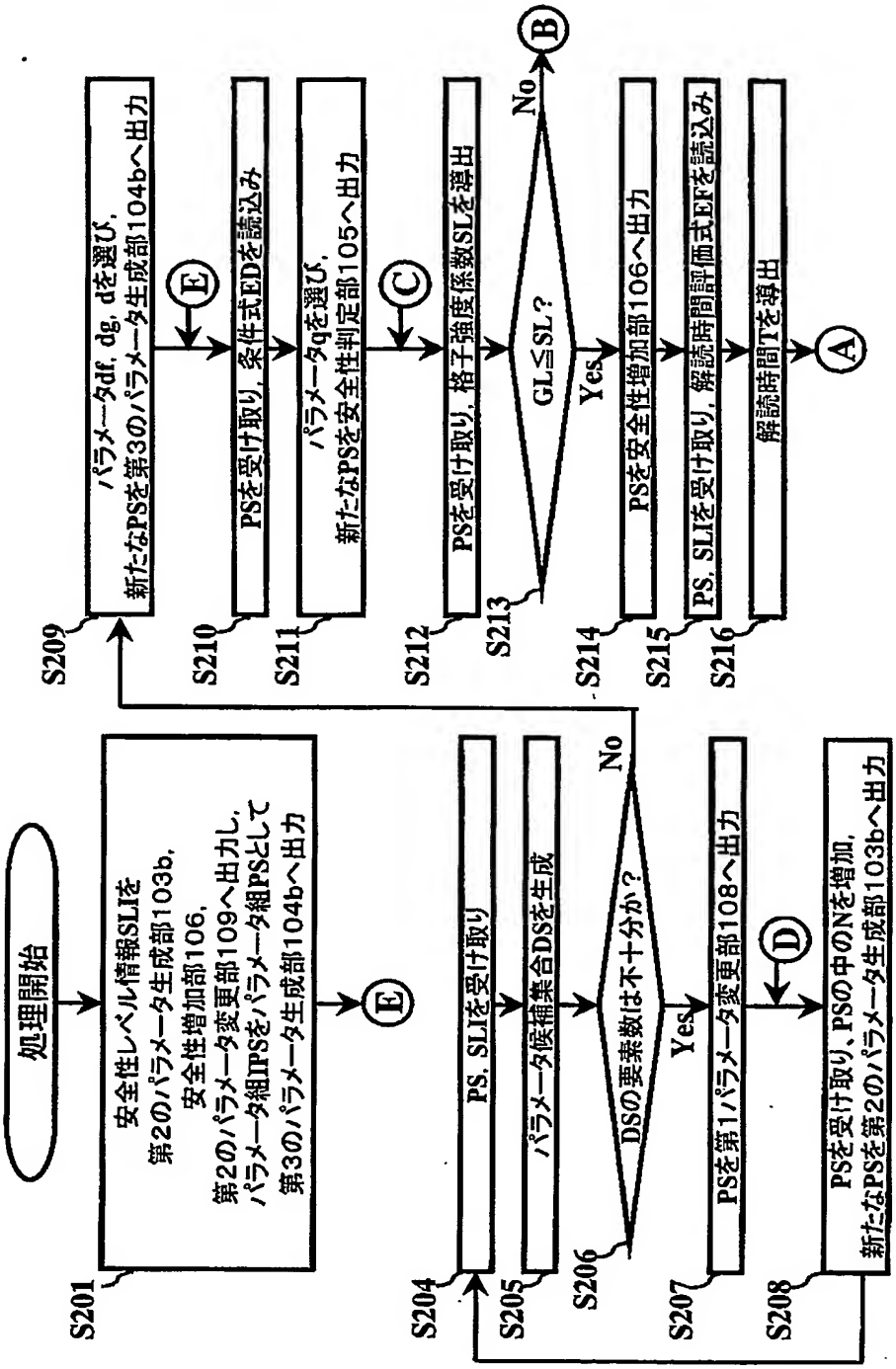
【図５】


A
T<SLI?
No
Yes
S117
T≧SLIとなるようにNを増加，新たなPSを生成
S118
Nは素数？
Yes
No
S119
Nが素数となるように増加し，新たなPSを生成
S120
PSを出力部107へ出力
S121
PSを出力
S122
処理終了
B
PSとSLIを受け取り，DSを生成
S123
dg＜M?
No
Yes
S124
dgを増加し，新たなPSを生成
S125
C
PSを第1のパラメータ変更部108へ出力
S126
D

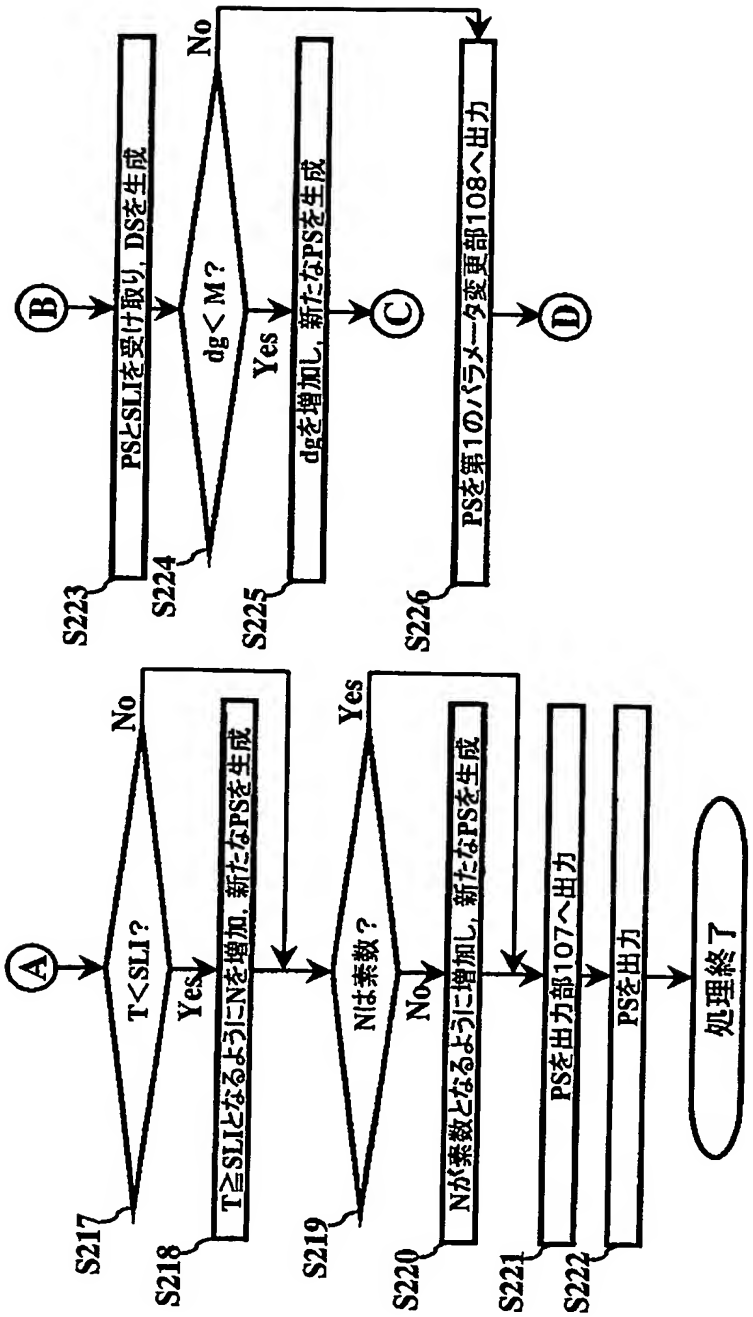
【図６】


2
パラメータ変換装置
入力部
101b
出力部
107
安全性増加部
196
第1のパラメータ変更部
108
第2のパラメータ変更部
109
第2のパラメータ生成部
103b
第3のパラメータ生成部
104b
安全性判定部
105
弐格納部
110
SLI
IPS
PS

【図７】


処理開始
安全性レベル情報SLIを
第2のパラメータ生成部103b,
安全性増加部106,
第2のパラメータ変更部109へ出力し,
パラメータ組IPSをパラメータ組PSとして
第3のパラメータ生成部104bへ出力
S201
E
PS, SLIを受け取り
S204
パラメータ候補集合DSを生成
S205
DSの要素数は不十分か？
No
Yes
S206
PSを第1パラメータ変更部108へ出力
S207
D
PSを受け取り、PSの中のNを増加,
新たなPSを第2のパラメータ生成部103bへ出力
S208
パラメータdf, dg, dを選び,
新たなPSを第3のパラメータ生成部104bへ出力
S209
E
PSを受け取り, 条件式EDを読込み
S210
パラメータqを選び,
新たなPSを安全性判定部105へ出力
S211
C
PSを受け取り, 格子強度係数SLを導出
S212
GL≦SL？
No
Yes
S213
B
PSを安全性増加部106へ出力
S214
PS, SLIを受け取り, 解読時間評価式EFを読込み
S215
解読時間Tを導出
S216
A

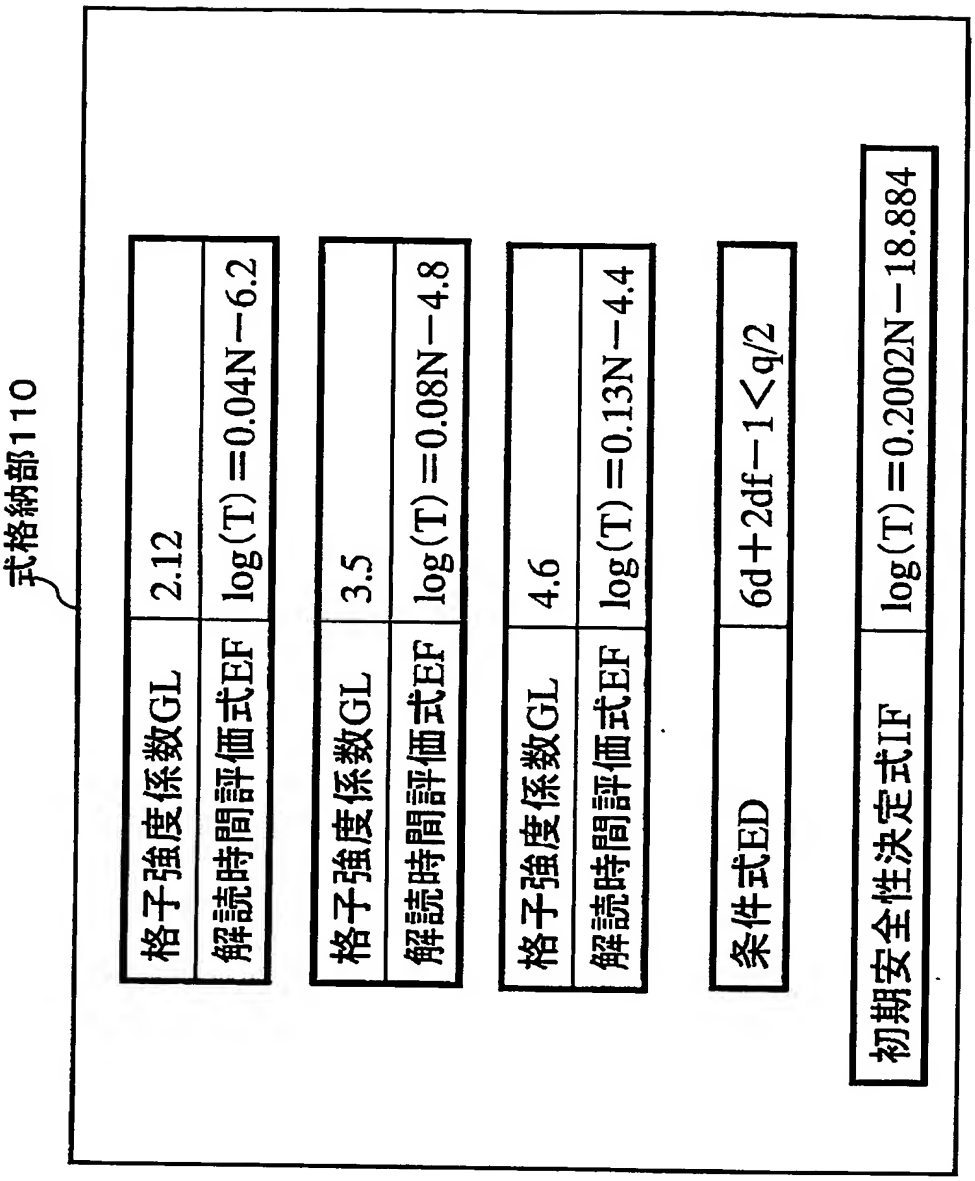
【図８】


B
PSとSLIを受け取り，DSを生成
S223
No
dg＜M？
Yes
S224
dgを増加し，新たなPSを生成
S225
C
PSを第1のパラメータ変更部108へ出力
S226
D
A
T＜SLI？
No
Yes
S217
T≧SLIとなるようにNを増加．新たなPSを生成
S218
Nは素数？
Yes
No
S219
Nが素数となるように増加し，新たなPSを生成
S220
PSを出力部107へ出力
S221
PSを出力
S222
処理終了

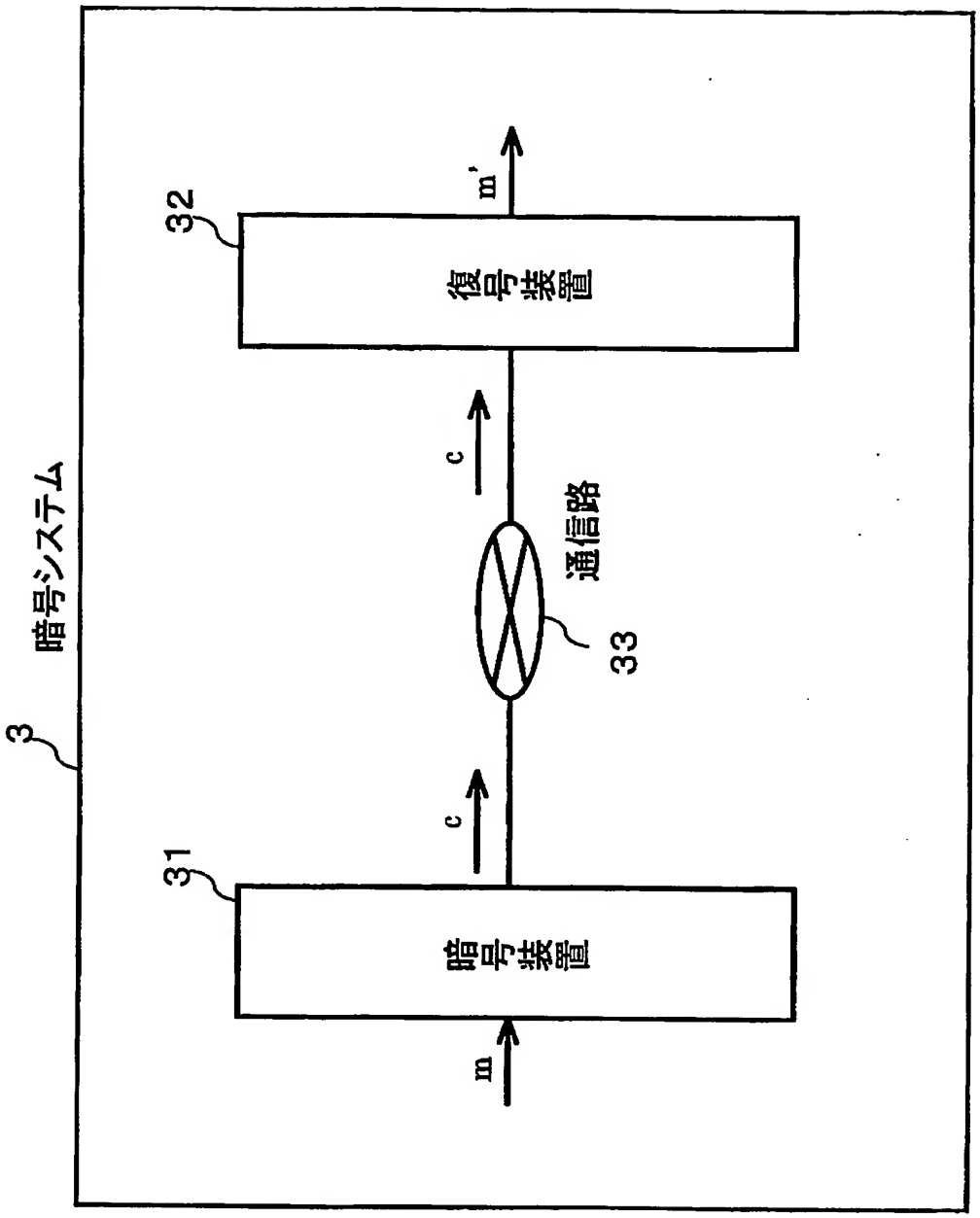
【図９】

安全性レベル情報SLI	パラメータ組IPS
512bit RSA暗号相当	IPS=(167,3,128,61,280,18)
1024bit RSA暗号相当	IPS=(263,3,128,50,24,16)
2048bit RSA暗号相当	IPS=(503,3,256,217,72,55)
:	:

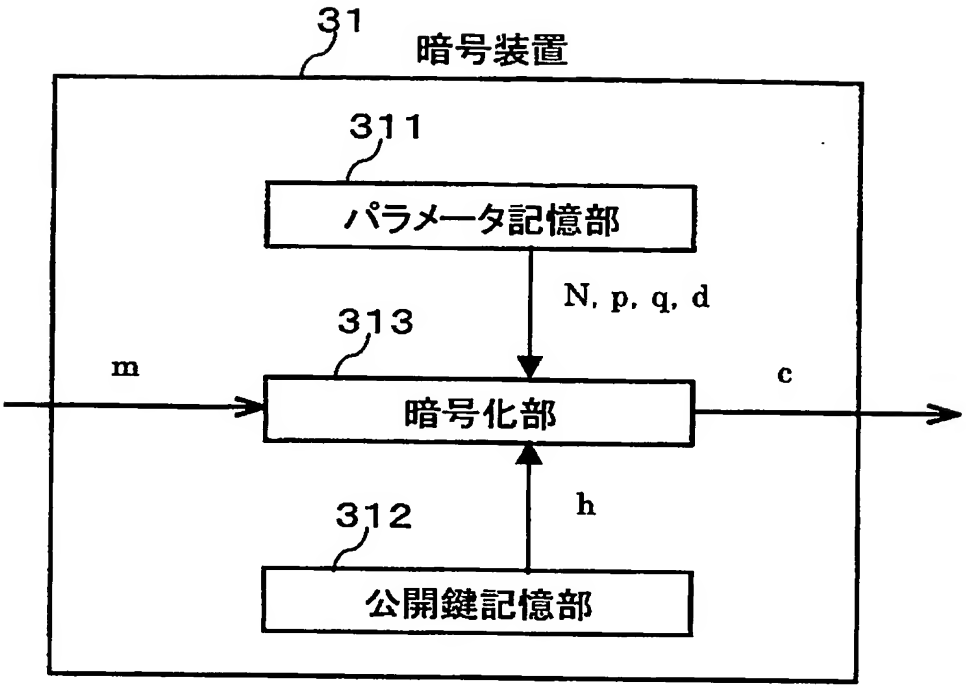
【図１０】


式格納部110
格子強度係数GL
2.12
解読時間評価式EF
log(T)＝0.04N－6.2
格子強度係数GL
3.5
解読時間評価式EF
log(T)＝0.08N－4.8
格子強度係数GL
4.6
解読時間評価式EF
log(T)＝0.13N－4.4
条件式ED
6d＋2df－1＜q/2
初期安全性決定式IF
log(T)＝0.2002N－18.884

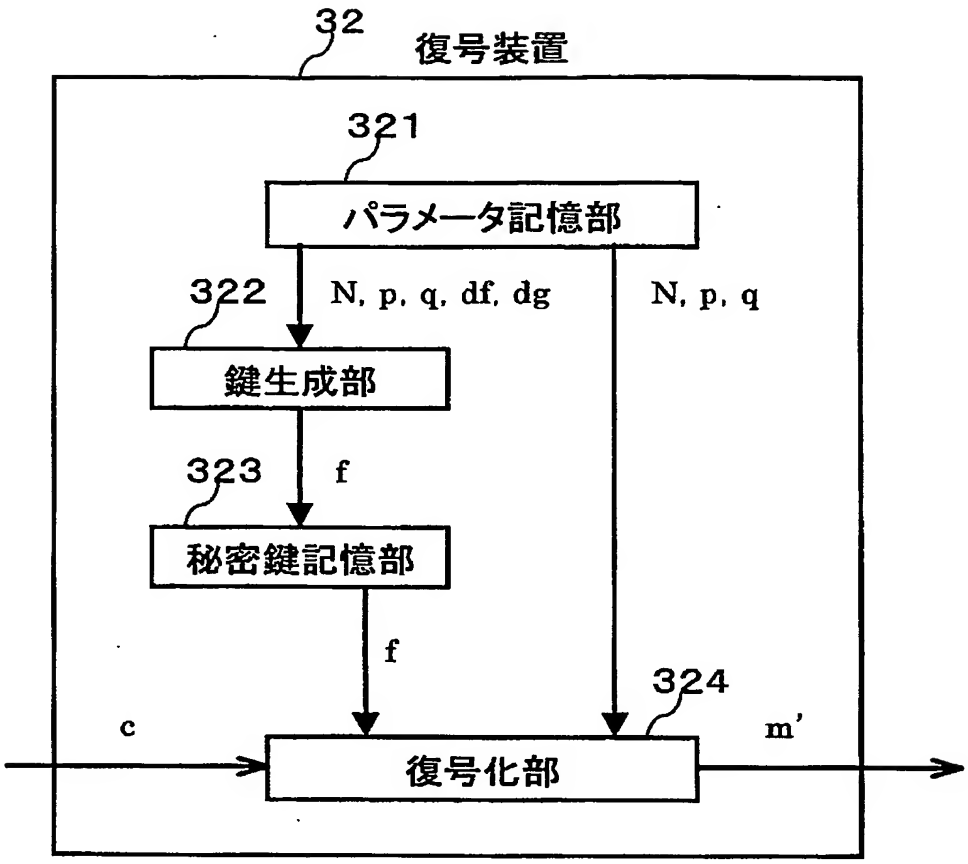
【図１１】



【図１２】



【図１３】


32
復号装置
321
パラメータ記憶部
322
N, p, q, df, dg
N, p, q
鍵生成部
323
f
秘密鍵記憶部
f
324
c
m'
復号化部

【書類名】　要約書

【要約】

【課題】　第三者による暗号解読に対して安全であり、かつ復号エラーが発生しないＮＴＲＵ暗号のパラメータを生成するための条件が知られておらず、そのようなＮＴＲＵ暗号のパラメータを生成できない。

【解決手段】　外部から入力された安全性レベル情報に基づき、前記安全性レベル情報の表す安全性を達成し、かつ復号エラーの発生しないＮＴＲＵ暗号のパラメータ組である出力パラメータを生成して出力するパラメータ生成装置であって、予め与えられた復号エラー発生有無を判定するエラー条件情報に基づいて、復号エラーが発生しない仮パラメータ組を生成する仮パラメータ生成部と、仮パラメータ組から格子強度係数を計算する格子強度係数計算部と、格子強度係数と安全性レベル情報に基づき、仮パラメータ組から出力パラメータを生成する出力パラメータ生成部とを備える。

【選択図】　図１

特願２００３－１１９９７３

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社